Rail Industry Visual Safety & Security Systems Strategy

A journey to a new future

Capgemini · NetworkRail · British Transport Police · Rail Delivery Group · National Rail · Rail Safety and Standards Board · DFTO Operator

April 2026

Table of Contents

Document navigation

1. Executive Summary

3. Future Roadmap

Technical and Functional Requirements

VSS Strategic Pillars

5. Technology Transformation

Why we need a VSS Strategy

What the Future VSS looks like

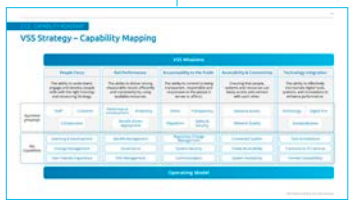
How to transform

2. VSS Vision, Missions and Enabling Priorities

4. Business Transformation

Case for Change

Capability Roadmap



6. Deep Dive Appendix *(Detailed Solution)*

Technical Architecture

Future Tech Trends

Implementing AI VSS Machine Vision

Economic Assessment

RAID

Glossary

Foreword

For two centuries, the railway in Great Britain has been at its best when it has embraced new technology to improve the service we provide. We have a proud history of using innovation to keep people safe, to run a more reliable railway and to support the communities and economy we serve every day.

Visual technology is central to that story. From the first cameras installed at a London station in the early 1960s – the world's first use of CCTV on the railway – we have steadily expanded and upgraded our systems. Today, cameras, control rooms and other visual tools are fundamental to how we protect passengers and colleagues, manage our assets and respond when things go wrong.

But the world has moved on. The quality of images, the power of networks and the potential of artificial intelligence have advanced dramatically. That creates a real opportunity to remove barriers between systems that have grown up separately across different organisations, and to strengthen how we support our customers and the operational performance of the railway.

This strategy sets out how we intend to seize that opportunity. Our ambition is to connect today's many separate visual systems and unlock the insight they hold. Done well, this will mean better decisions and swifter action when incidents occur – a tangible contribution to delivering a simpler, better railway.

We are equally clear about the risks. Visual technologies offer powerful new capabilities, from high-quality video to AI-enabled analytics, but they also raise important questions about cybersecurity, privacy and the resilience of systems that are becoming critical infrastructure. Our response is to focus first on the foundations: the quality of images we capture, and the secure connectivity needed to share them across the network.

Although this strategy is about visual safety and security systems, its purpose is broader. At its heart, it is about better outcomes for everyone who depends on the railway – passengers, freight customers, lineside neighbours and our own colleagues. By improving visibility across the network, we can prevent more incidents and respond more effectively when they do occur.

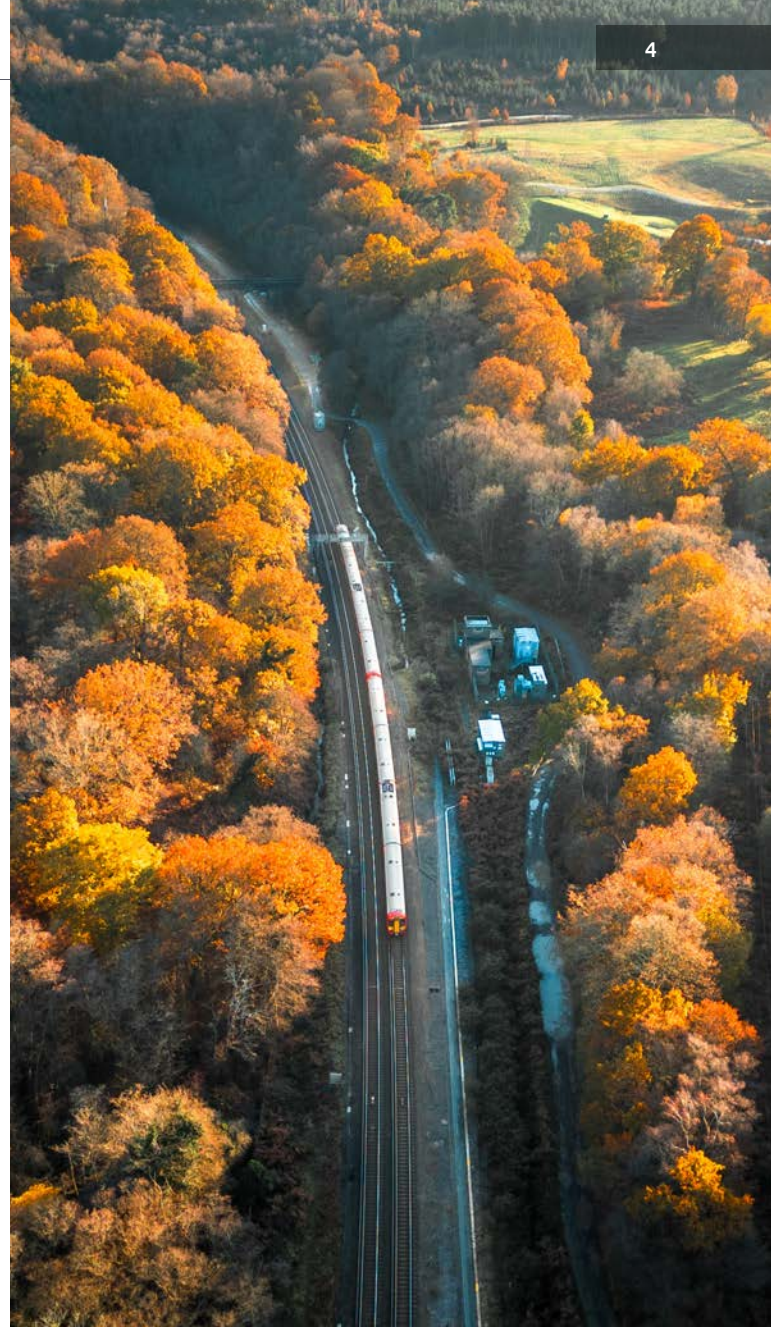
Setting out this strategy is only the start. Delivering it will depend on close partnership across the industry. We want to encourage all those with a stake in Britain's railway to engage with what is set out here, challenge it, help shape the priorities and play an active part in putting it into practice. If we get this right together, we will strengthen the safety and performance of the railway today and build the foundations for what comes next.

Alex Hynes

Chief Executive of DfT Operator

Jeremy Westlake

Chief Executive of Network Rail



This Strategy has been shaped and developed by the industry, for the industry

Thank You

We would like to extend our sincere thanks to all the industry partners and stakeholders who generously contributed their time, insights, and expertise throughout the development of the VSS Strategy.

Your input has been invaluable in forging a direction that is both ambitious and grounded in real-world needs.

This Strategy reflects the priorities and aspirations you shared and is committed to translating your feedback into meaningful action. Your collaboration has not only informed this Strategy's development, but it has also made it possible.

We look forward to continuing this partnership, and we remain grateful for your ongoing support.

1 Executive Summary

The VSS industry Strategy sets out a joint industry vision to harness the power of railway visual safety and security systems (VSS) to deliver a railway that serves everyone. By focusing on safety and performance, we make rail the preferred choice, enhance customer satisfaction, and build a more affordable, sustainable future for all.

It aims to define a better-connected and smart VSS that delivers tangible benefits for passengers, the public, staff, and stakeholders.

While legacy systems, fragmented governance, and inconsistent deployment have presented challenges to current VSS capabilities, this Strategy introduces a unified path designed to build on the progress made to date, aligning the industry for greater impact today and preparing it for GBR tomorrow.

The Strategy takes a holistic approach by making recommendations for the entire VSS Operating Model, with a key focus on people and technology, including best practice design principles, integration routes, and a scalable, AI-enabled architecture.

There are three key themes for this technological change, which include Quality, Connectivity, and Coverage (QCC).

Serving as a common reference point, the Strategy guides VSS business and asset owners on how to plan future investments, select the right technology, break down barriers between organisations, and coordinate upgrades, renewals, and deployments of VSS solutions both immediately and in the future. It acts as an accelerator for a pragmatic and organic industry-wide VSS evolution that starts today and will shape the next decade of transformation.

Confidence in this strategic direction is expected to unlock investment, foster adaptability, and strengthen connectivity and collaboration across the industry. Financial modelling based on operational data indicates potential savings of up to £20 million in Schedule 8 costs per annum and an estimated £16 million per annum in safety-related savings, lower OPEX costs and a range of other benefits – to be realised following the implementation of the Strategy.

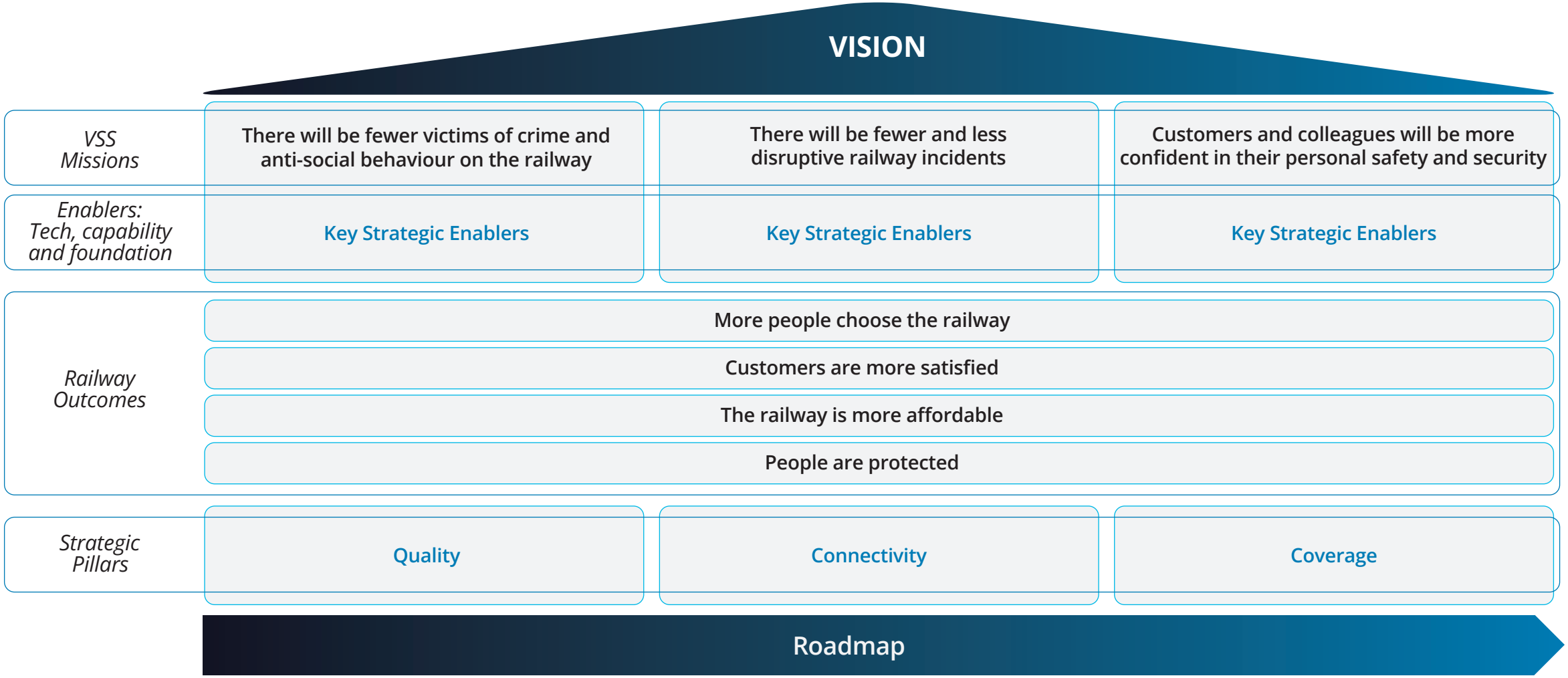
With executive endorsement already secured, the Strategy is now ready to be delivered. This is the time to capitalise on the support and desire for change. Stakeholders are encouraged to engage with the technology recommendations, capability roadmap, and prioritised next steps to drive the Strategy forward, together.

1.2 VISION STATEMENT

We are driven by a joint industry vision to unlock the full potential of VSS systems

We harness the power of railway visual safety and security systems (VSS) to create a railway that serves everyone. By prioritising safety and performance, we make rail the preferred option, improve customer satisfaction, and build a more affordable sustainable future for all.

The strategy is structured to begin with a clear vision and cascade down through VSS Missions, enablers, outcomes, and strategic pillars.



Key strategic enablers:
Strengthening Railway Security

There will be **fewer victims of crime** and **anti-social behaviour** on the railway

- Put cameras in places that are more likely to have incidents, so we can help prevent them from happening.
- Connect video systems to BTP to help them respond faster to crime incidents and allow them to gather evidence quickly.
- Make sure the video is clear enough to see who did what, which helps with police investigations.
- Use smart systems to proactively warn staff when something unsafe is happening, which helps prevent major escalations.
- Give control rooms anywhere in the country a clear view of what's happening on the network so incident responses can be better organised.
- Let authorised staff watch live video so they can quickly spot and deal with issues.

Rail Outcomes:

MORE PEOPLE CHOOSE THE RAILWAY	CUSTOMERS ARE MORE SATISFIED	THE RAILWAY IS MORE AFFORDABLE	PEOPLE ARE PROTECTED
Encourage a greater number of passengers to opt for rail over alternative transport.	Consistently meet customers' expectations and needs through quality experience.	Reduce incidents costs in the railway, which makes it more affordable.	Strengthen people's personal safety and security across the rail network.

Key strategic enablers:
Unlocking Greater Performance

There will be **fewer and less disruptive railway incidents**

Allow BTP to view footage instantly so train services can get back to normal as quickly as possible after an incident.

Install and upgrade cameras in places where problems are most likely to cause disruptions.

Analyse video data from past incidents to create new ideas for protecting the railway.

Use clear and live/recorded video as a means for Network Rail, BTP, Train Operating Companies and Partners to work together when managing incidents.

Ensure video systems are secure and reliable, so they are always available when they are needed.

Use common technology and methods everywhere to make handling incidents smoother and more consistent.

Rail Outcomes:

MORE PEOPLE CHOOSE THE RAILWAY
Encourage a greater number of passengers to opt for rail over alternative transport.

CUSTOMERS ARE MORE SATISFIED
Consistently meet customers' expectations and needs through quality experience.

THE RAILWAY IS MORE AFFORDABLE
Reduce incidents costs in the railway, which makes it more affordable.

PEOPLE ARE PROTECTED
Strengthen people's personal safety and security across the rail network.

Key strategic enablers:
Driving People Safety

Customers and colleagues will be **more confident** in their **personal safety and security**

Make sure cameras are covering high-risk areas to help identify issues before they can cause harm, injuries or hazards.

Allow control rooms to access live video and respond quickly to emergencies, suspicious behaviour, or safety hazards.

Train staff on how the systems work, so they can benefit from the new capabilities, which increases their confidence in doing their jobs well.

Protect recorded footage from unauthorised access or misuse, in line with data protection laws.

Help protect customers and staff from abuse or aggression by making it clear they can record video evidence from a range of cameras.

Rail Outcomes:

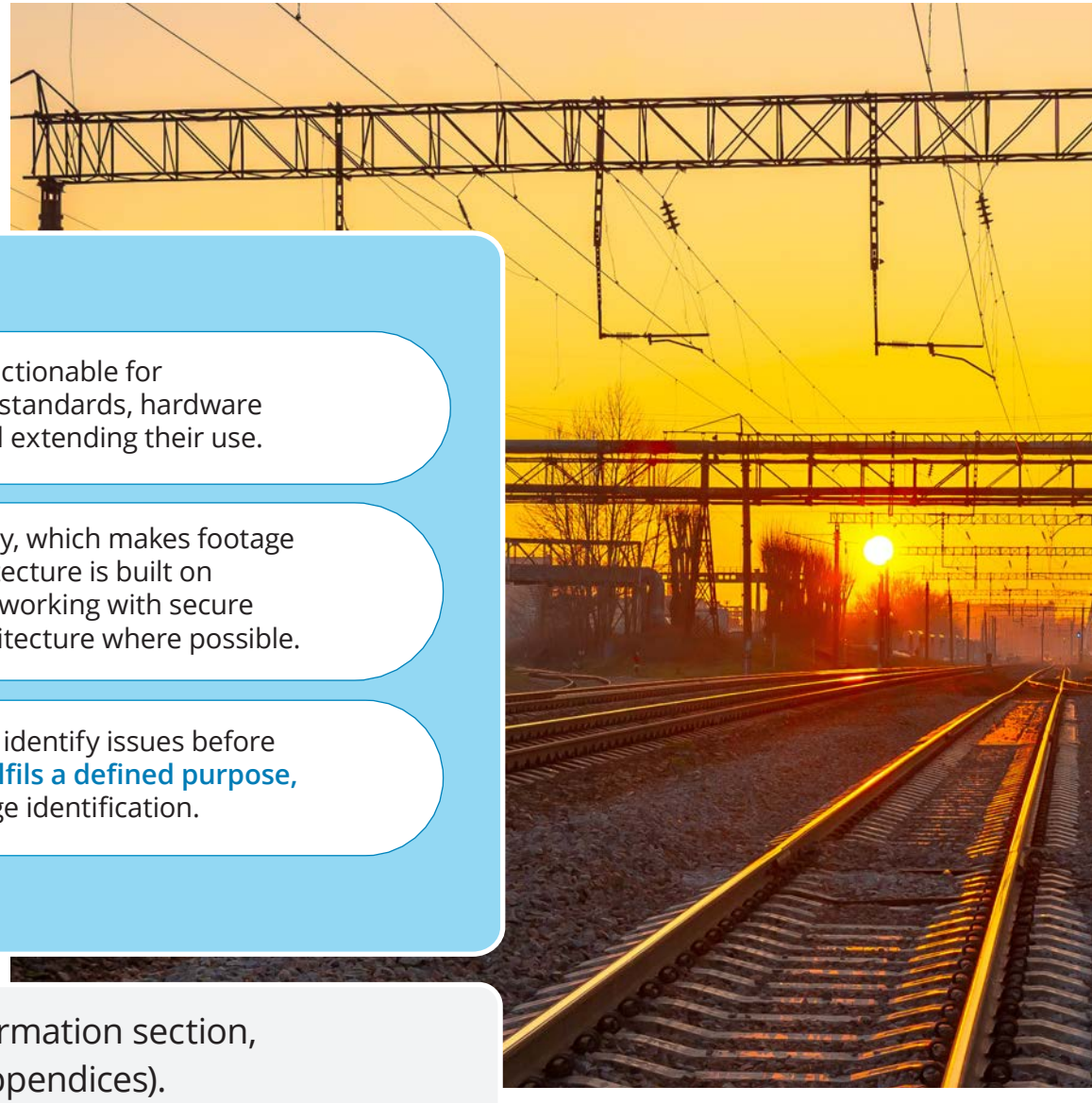
MORE PEOPLE CHOOSE THE RAILWAY
Encourage a greater number of passengers to opt for rail over alternative transport.

CUSTOMERS ARE MORE SATISFIED
Consistently meet customers' expectations and needs through quality experience.

THE RAILWAY IS MORE AFFORDABLE
Reduce incidents costs in the railway, which makes it more affordable.

PEOPLE ARE PROTECTED
Strengthen people's personal safety and security across the rail network.

The VSS Strategic Pillars are the foundations on which future solutions will be built, and current solutions will be assured



VSS strategic pillars

QUALITY

Ensuring that **visual information and data remain clear,** reliable and actionable for operational and analytical use. The strategy will lead to clear technical standards, hardware and software requirements for VSS systems, increasing their value and extending their use.

CONNECTIVITY

New systems will have more secure and high-performance connectivity, which makes footage rapidly available for people while also protecting it. The strategic architecture is built on a **resilient, layered connectivity model** that combines on-premise networking with secure cloud pathways. Cybersecurity is embedded through a Zero Trust architecture where possible.

COVERAGE

The solution ensures that cameras are covering high-risk areas to help identify issues before they can cause harm, injuries or hazards. This means **every camera fulfils a defined purpose,** whether for wide-area detection, situational observation, or close-range identification.

The VSS solution pillars are outlined in the Technical and Business Transformation section, with the corresponding architecture provided in the Deep Dive section (Appendices).

Building the Future of VSS: *A roadmap for a securely connected infrastructure that can be enhanced with the latest technology over time*

This roadmap explains how the railway can go through a pragmatic transformation journey which is fast-paced, realistic and sustainable.

1 **PHASE 1** — **2026–2027**

2 **PHASE 2** — **2028–2029**

3 **PHASE 3** — **2030–2034**

This roadmap represents an ongoing journey of continuous improvement, and the activities are not linear. The industry will evolve by developing core business and technology capabilities, strengthening systems and architecture, which will allow the industry to sustainably implement intelligent technologies over the coming years.

CP7

We will improve the current VSS systems and, through this strategy, agree on a common architecture, consistent standards and the future target state.

We will connect and integrate VSS systems to provide a single environment that provides visibility to the right places and democratises access to the right people at the right time.

A list of initiatives can be found in the **Business Transformation** section – **Capability Roadmap**

CP8

We will adopt and embed even more new technologies to increase the value of VSS, supporting railway workers, security partners and our passengers.

The list of future **Tech and Capabilities** for this phase can be found in the **Future Tech** section

2 BUSINESS TRANSFORMATION

SECTION TAKEAWAYS: This section outlines the Strategic Business imperative for change, presenting a case for transformation driven by opportunities to drive great value. It articulates the VSS vision for a reimagined operating model and introduces a structured capability roadmap that prioritises key initiatives across people, processes, and technology. The roadmap serves as a phased guide to building capabilities.

2.1.1

CASE FOR CHANGE

SECTION TAKEAWAYS:

The Strategy clearly defines the VSS industry problem statement and challenges. It provides an opportunity to shape the next generation of safety-critical infrastructure. This section not only outlines the critical priority considerations to address and mitigate against upfront, but also reveals opportunities that represent practical levers for delivering value.

2.1.1 A PROBLEM STATEMENT

The Case for Change: *Why we must act now*

This is an opportunity to support safety and security activities to achieve better overall outcomes.

The Current Situation: A One-Time Window of Opportunity

The rail industry is entering a decisive period for technology investment across the network.

Renewals and infrastructure projects currently underway represent a unique opportunity to future-proof critical systems. **Now is the time to align infrastructure upgrades with a forward-compatible Strategy.**

Once deployed, assets typically remain in place for 7–15 years, **so decisions and deployments made today will shape the operational and digital capabilities of the railway well into the future.**

Towards a Safer, Smarter and More Secure Railway

Modern VSS Systems are no longer passive assets – they are critical enablers of safer, more secure, and performance-driven rail operations.

Enhanced systems will allow for proactive incident detection and intervention, along with faster recovery from, and a reduction in, safety-related incidents, which in turn minimises delays while improving service reliability.

This not only delivers better value for public money but also strengthens passenger and staff confidence in safety.

Enabling Tomorrow's Capabilities

The VSS Strategy positions the rail network to take advantage of emerging technologies.

These capabilities support a transition from reactive systems to intelligence-led network resilience – aligned with wider industry ambitions on improved safety, security and rail performance.

Understanding the Landscape of VSS in Rail Today

To inform a future-ready approach to VSS systems, it is essential to establish a clear, industry-wide baseline of how these capabilities are currently structured, governed, and applied across the UK rail network.

This section sets out a strategic overview of the existing landscape – highlighting how VSS is used, who holds responsibility for its deployment and operation, and the extent to which current systems support the evolving needs of the rail industry.

By understanding today's foundations, the rail industry can more effectively shape a modern, intelligent, and interoperable VSS ecosystem for the future.

What VSS Means in Today's Railway

Visual Safety & Security (VSS) systems in the UK rail industry encompass a broad ecosystem of technologies designed to enhance the safety, security, and operational resilience of the network. Far beyond traditional CCTV, VSS now incorporates a diverse range of data-rich visual sources that enable real-time situational awareness and smarter decision-making.

VSS capabilities include:

- Fixed and mobile camera systems, including:
  - Stationary CCTV at stations, crossings, and depots.
  - Front-facing and on-board train cameras.
  - Body-worn video is used by staff and security teams.
  - Drone footage for overhead inspection and incident response.
- Integrated Cloud-Based VSS for live monitoring, storage, and retrieval.
- Sensor and analytics tools to support automation, incident detection, and AI-powered analysis.

Use cases span:

- Safety and security monitoring at high-risk or operationally sensitive locations.
- Asset condition monitoring for early detection of faults, environmental risks, or structural issues.
- Passenger flow, crowd dynamics, and dwell time analytics to optimise customer experience.
- Post-incident investigation and evidence gathering for enforcement or claims management.

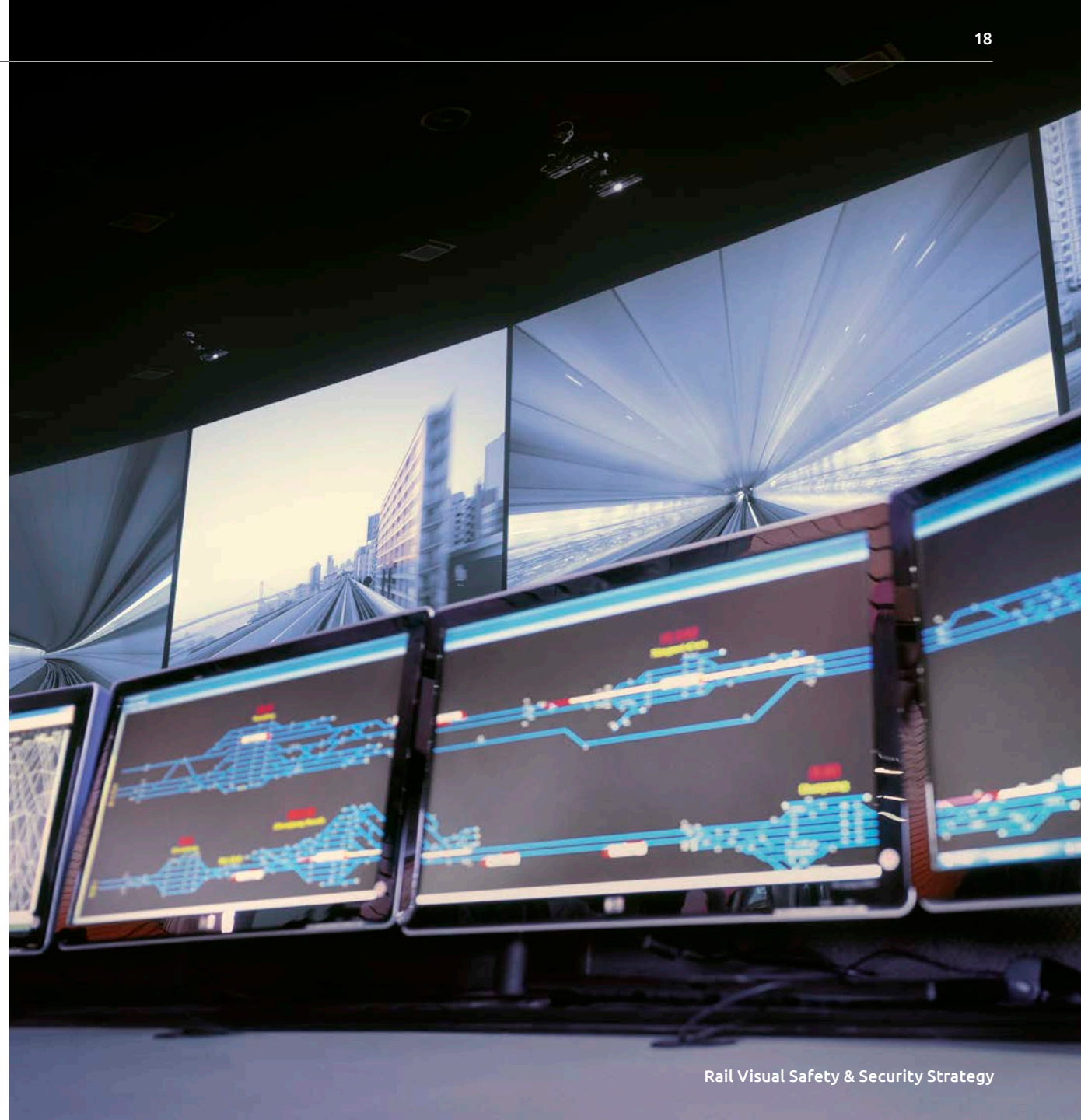
The scope of the VSS strategy covers both safety and security use cases, which are broad themes with a range of cameras and systems. For further details, please find the scope of the strategy in the Appendix (page 52).

2.1.1 B CURRENT STATE | Current State Assessment

Key Roles Across the Industry VSS Ecosystem

The delivery and oversight of Visual Safety & Security (VSS) systems in the UK rail network is shared across multiple stakeholders. Each plays a distinct role in shaping how visual data is captured, accessed, and used to support a safer, more intelligent railway.

Organisation	Role in VSS
Network Rail	Owns and manages the majority of fixed VSS infrastructure at managed stations and across trackside assets. Operational responsibility is devolved to Regional Telecoms Asset Performance Managers (RTAPMs).
Train Operating Companies *(TOCs)*	Responsible for onboard VSS systems (e.g. front-facing, saloon, and driver-view cameras). In some cases, TOCs also manage station-based systems in leased or franchised locations.
British Transport Police *(BTP)*	Principal user of VSS outputs for safety, threat detection, incident response, and post-event investigation. Integration with BTP platforms is essential for maximising system value.
Station Facility Operators *(e.g. Merseyrail)*	Manage VSS systems at non-Network Rail operated stations. These often follow differing technical architectures, operational models, and integration levels.
Infrastructure Contractors and Maintainers	Operate or monitor VSS as part of infrastructure maintenance contracts (e.g. for remote asset monitoring).
Technology Suppliers & Vendors	Provide hardware, software, installation, and in some cases manage outsourced security services.



Current VSS Systems and Services in Practice

Current Asset and Service Overview

VSS assets are spread across thousands of locations, and many assets have been installed piecemeal over 25+ years, resulting in mixed levels of technological maturity – from analogue systems to digital and AI-enabled platforms.

Network Coverage: VSS capabilities are deployed across stations, platforms, level crossings, depots, onboard rolling stock (including front-facing and saloon cameras), and trackside infrastructure.

Technology Landscape: The current estate reflects more than two decades of incremental investment. As a result, the network includes a wide spectrum of technologies - from legacy analogue systems to fully digital, AI-enhanced platforms capable of intelligent detection and real-time alerting.

Data Flow and Accessibility: The ability to share and act on VSS data depends heavily on local infrastructure:

- Advanced sites are now able to stream high-resolution footage in real time to British Transport Police, Network Rail and TOC operations centres.
- In contrast, many locations still require manual extraction of footage (e.g., hard drives, USB sticks), limiting the speed and effectiveness of incident response.

This fragmented landscape reinforces the need for coordinated investment, common technical standards, and a strategic roadmap to unlock the full value of VSS technologies.

Area	Current State
Ownership	Dispersed across Network Rail, Train Operating Companies (TOCs), and third-party providers, with no unified asset register.
Governance	Responsibility for oversight and investment is devolved; the industry lacks a central governance model for VSS.
System Maturity	Technology varies widely - ranging from legacy analogue setups to modern, AI-enabled digital platforms.
Use Cases	Deployed to support public and staff safety, asset condition monitoring, and operational intelligence (e.g. crowd flow).
Access & Integration	Access rights and system interoperability are fragmented, limiting real-time data sharing and consistent use across stakeholders.

Today's VSS landscape is rich but inconsistent, with strong foundations in safety and operational effectiveness.

The VSS estate initially met its purpose, but over the past 20 years, technology has evolved significantly, creating new opportunities to exploit.

Various stakeholders, including BTP and TOCs, interact with Network Rail's VSS, and ownership of assets is divided across various parties.

Trespass, suicide and vulnerable presentations resulted in Network Rail incurring ~£160m in Schedule 8 costs for FY23/24, of which legacy VSS systems were a contributing factor.

While the technology is already making a difference across many parts of the network, the current structure - defined by fragmentation and decentralisation - presents a compelling opportunity for greater alignment, standardisation, and strategic uplift. This Strategy aims to build on what works well, while defining a clearer path forward for the entire industry.

Built with the Industry

This Strategy has been developed in close collaboration with partners across the rail industry, drawing on the expertise of subject matter specialists and operational stakeholders.

Stakeholder Engagement

Engagement included structured interviews, workshops, and data collection from a broad spectrum of industry representatives - ensuring the Strategy reflects shared ambitions, addresses practical challenges, and considers the diverse needs across the network.

Literature Review

An extensive review of industry literature, guidance documents, and technical specifications was also undertaken. These sources provided vital context on current standards and policies, helping to shape a forward-looking Strategy that builds on, but more importantly, goes beyond legacy approaches.

This collective input has been instrumental in identifying key opportunities, blockers, and risks to successful implementation - ensuring the Strategy is not only visionary, but grounded in real-world deliverability.

2.1.1 C STRATEGIC ALIGNMENT

One Vision, Many Tracks: *Aligning across the Rail Industry*

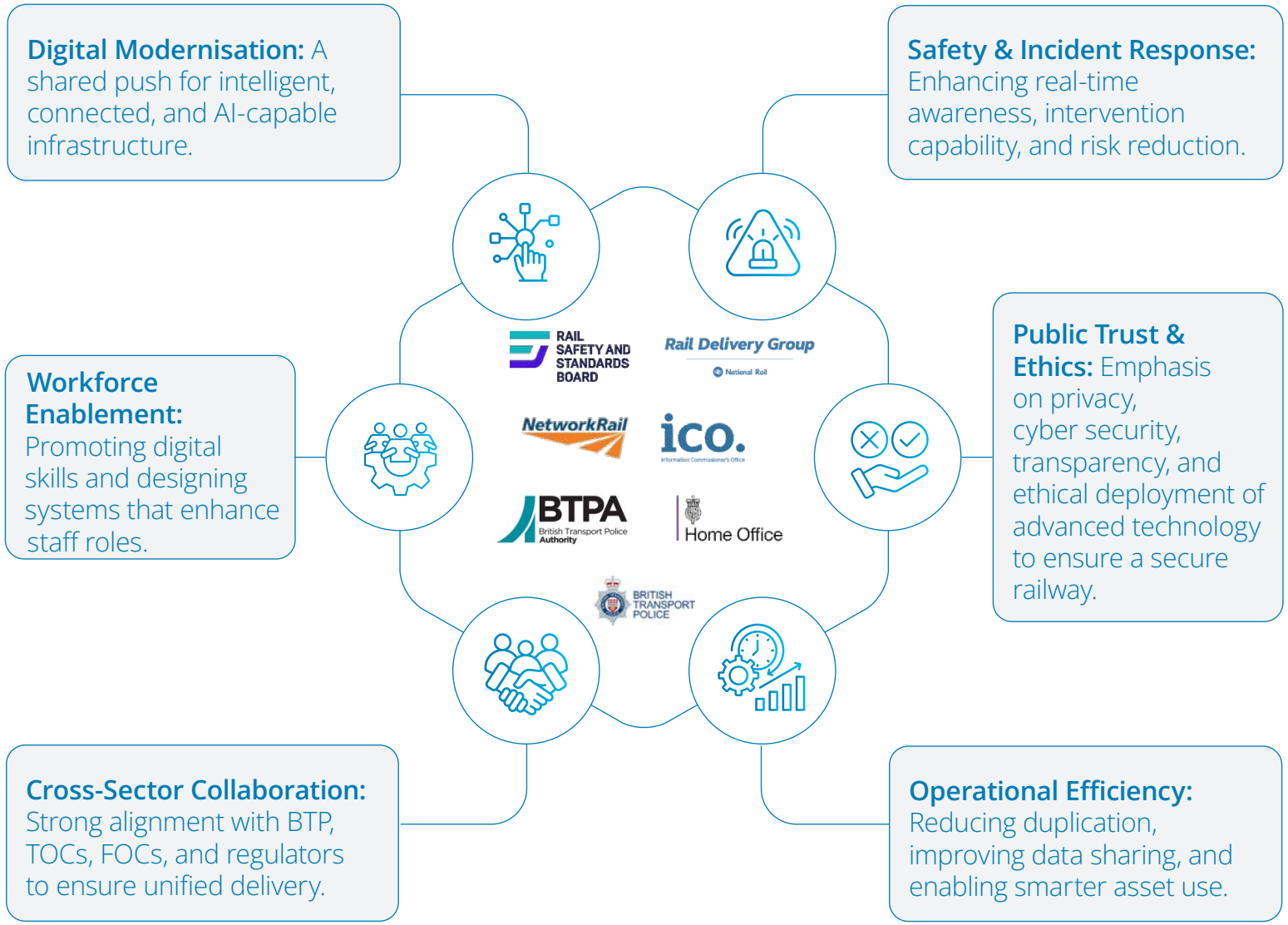
To drive lasting impact, the VSS Strategy aligns with wider industry goals across safety, security and rail performance. This ensures the Strategy is built on shared priorities.

While the VSS Strategy draws on a range of existing industry documents - some of which are now outdated – it is not built on these legacy standards.

Rather, they were reviewed for contextual understanding of policy direction and used alongside interviews, workshops, and other industry-wide inputs to inform a plan for a future that goes beyond the current As-Is estate with smarter and more intelligent infrastructure.

This Strategy is grounded in reality but designed to significantly move the Rail industry forward and set it up for a future that reflects industry priorities around safety, security and enhanced rail performance.

For a more detailed review of the Strategy alignment, please see the Deep Dive (Appendices) section.



Clearing the Path Ahead: *Navigating Risks, Constraints and Dependencies*

To successfully deliver this Strategy, it's essential to understand and manage the risks and constraints that could hinder progress, as well as the key dependencies it relies upon.

This section outlines only the critical priority considerations to address and mitigate upfront. A full log of risks, constraints and dependencies is available in the Deep Dive (Appendices) section.

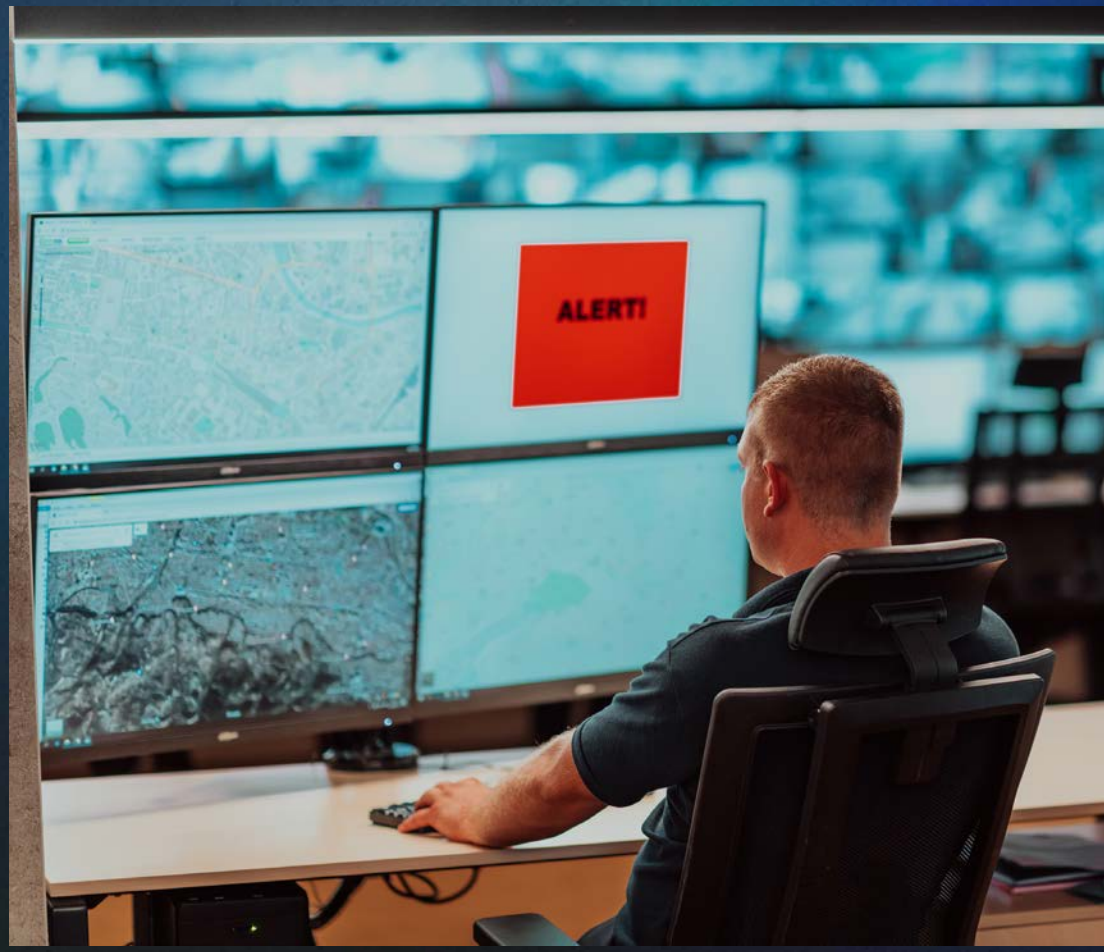
CATEGORY	DESCRIPTION	MITIGATION/ACTION
Risk	**FUNDING** Securing funding for asset renewals and enhancements could be a challenge, as the industry is constrained regarding the current funding position for CP7, which may lead to delays or compromises in project scope.	Develop a VSS business case highlighting the long-term benefits and cost savings of the programme to secure necessary funding from stakeholders and potential funders. Develop a renewal-based Capability Roadmap which is flexible allowing capability growth as and when funding is available. Look at alternatively funding models/ servitisation to reduce cost may also help mitigate this.
Dependency	**EXTERNAL STAKEHOLDER BUY IN** Dependency on the rail industry stakeholders to drive the implementation and technical changes of the VSS Strategy to enable VSS improvements across the rail industry.	As part of the Strategy development, establish a Steering Group and engage with Task & Finish Groups. Conduct 1:1 interviews with key industry stakeholders to secure alignment.
Dependency	**EFFECTIVE STRATEGY DELIVERY & IMPLEMENTATION HANDOVER** Dependency on Network Rail's DDaT function, and any similar functions within TOCs and FOCs, to act as the primary delivery owners for Strategy implementation.	Successful transition from Strategy development to implementation relies on early and sustained engagement with National Rail DDAT and similar functions within TOCs and FOCs. Clear implementation governance structure proposed as part of the Strategy to maintain delivery momentum beyond development. Ensure DDaT and Technical Authority have a defined role in governance post-Strategy.
Constraint	**FUNDING UNCERTAINTY & PRIORITISATION** Elements of the Strategy implementation is constrained by capital investment windows tied to Control Periods (CP7, CP8); differing budget processes across entities.	Phased implementation aligned to financial and digital maturity. Use the Business Case to support prioritisation in capital allocation. Maintain proactive engagement with DfT, ORR, GBR Transition Team, and funders to influence forward planning and secure early commitment. Ensure the Strategy is synchronised with CP8 and future funding windows to maximise alignment with Network Rail and GBR investment plans.

Strategic Opportunities Ahead

This Strategy not only addresses the challenges facing the current VSS landscape but also reveals clear opportunities that can be explored. These opportunities represent practical levers for delivering greater value – both immediately and over the long term. This section outlines only the most transformational opportunities. A full log of all opportunities is available in the Deep Dive (Appendices) section.

DESCRIPTION	BENEFIT
UNLOCKING GOVERNMENT FUNDING The Strategy presents an opportunity to position VSS as a national infrastructure priority, helping unlock government innovation grants and green technology funding.	Reduces dependency on traditional funding cycles, accelerates implementation, and attracts investment.
PUBLIC & PRIVATE STAKEHOLDER BUY-IN There is an opportunity to enhance the Strategy business case by demonstrating long-term savings and improvements in safety, security, and performance, making it attractive to both public and private stakeholders.	Enhances the case for investment by demonstrating tangible value, increases likelihood of securing funding by being a key part of planning for future funding cycles.
IMPROVED BTP & LOCAL AUTHORITY COLLABORATION The Strategy presents an opportunity to develop connected systems that provide BTP and relevant Local Authorities with live access to critical feeds, enhancing situational awareness.	Enables faster incident response, improves situational awareness, which in turn helps reduce service disruptions and their associated costs. Supports a more proactive and coordinated approach to safety and security across the rail network.
GBR READINESS The Strategy presents an opportunity to align with and support the future GBR operating model by promoting consistency and interoperability in security infrastructure.	Helps industry partners transition effectively into GBR, reducing fragmentation and ensuring VSS systems are ready for integration into a unified rail governance model.

2.1.2 CAPABILITY ROADMAP



SECTION TAKEAWAYS:

Meet strategic aspirations. Leaders and Change Champions should use this roadmap to assess current maturity, identify gaps, and plan transformation journeys over the Phase one period *(indicative timeline from start of strategy implementation and the right governance put in place).* Capabilities which will have the most impact have been highlighted and prioritised.

Introduction

Capabilities within the VSS context

Capabilities are the **high-level abilities** that an organisation or industry **creates or enhances** to maintain momentum and pace of change. **Capabilities are built through an Operating Model,** which is a combination of people, processes, technology and governance dimensions. These are essential for executing a Strategy.

Development of the VSS Capability Roadmap

Following the discovery phase, which focused on understanding the needs of the rail industry, the industry defined a comprehensive set of **aspirations.** These aspirations were grouped into **five key pillars for the success of the VSS Strategy: 1.** People Focus **2.** Rail Performance **3.** Accountability to the Public **4.** Accessibility & Connectivity **5.** Technology Integration.

The industry has defined the capabilities it needs to deliver these aspiration groups and ultimately the **VSS Vision.** The capability map provides a comprehensive **list of priority abilities** for the industry to focus on over the next years. In addition, the sequence of the roadmap is aligned to the Industry priorities (**1.** Transition from Analogue to IP, **2.** Connectivity **3.** Artificial Intelligence).

To implement the Capability roadmap, organisations are encouraged to undertake a **capability maturity assessment** to review their current capabilities against the future state and then develop a change and transformation plan.

Value

This roadmap aligns the industry's long-term goals with the development of its core capabilities, **helping prioritise investments, manage dependencies,** and ensure that **resources are directed** towards impactful initiatives.

2.1.2 CAPABILITY ROADMAP

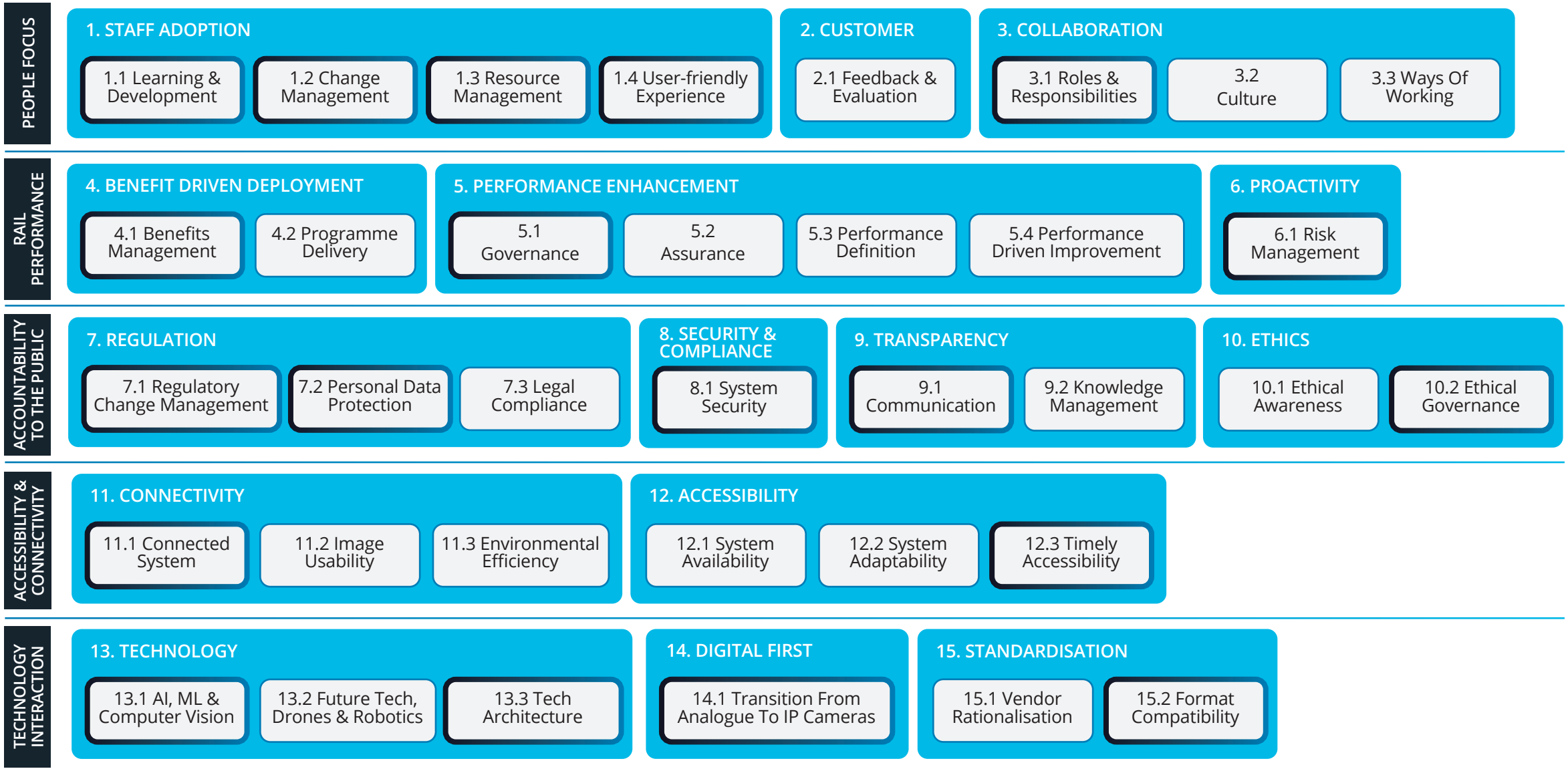
VSS Strategy – Capability Mapping

VSS Capabilities

	People Focus	Rail Performance	Accountability to the Public	Accessibility & Connectivity	Technology Integration
	The ability to understand, engage and develop people skills with the right training and resourcing Strategy.	The ability to deliver strong, measurable results efficiently and consistently by using available resources.	The ability to commit to being transparent, responsible and responsive to the people it serves or affects.	Ensuring that people, systems and resources can easily access and connect with each other.	The ability to effectively incorporate digital tools, systems, and innovations to enhance performance.
Aspiration groupings	Staff Customer Collaboration	Performance enhancement Proactivity Benefit-driven deployment	Ethics Transparency Regulation Safety & Security	Network Access Network Quality	Technology Digital first Standardisation
Key Capabilities	Learning & Development Change Management User-Friendly Experience	Benefit Management Governance Risk Management	Regulatory Change Management System Security Communication	Connected System Timely Accessibility System Availability	Tech Architecture Transition to IP Cameras Format Compatibility

Operating Model

Core Capabilities & Strategic Alignment



1 Developing capabilities around people

The ability to understand, engage and develop people skills with the right training and resourcing Strategy.

KEY: Aspiration group Level 1 | Capability Level 2 | Priority Capabilities

1. STAFF ADOPTION

- 1.1 Learning & Development
- 1.2 Change Management
- 1.3 Resource Management
- 1.4 User-friendly Experience

2. CUSTOMER

- 2.1 Feedback & Evaluation

3. COLLABORATION

- 3.1 Roles & Responsibilities
- 3.2 Culture
- 3.3 Ways Of Working

1.1 Learning and Development

Ability to identify and analyse the skills required for delivering the Strategy's vision. Highlights the ability to develop and maintain a plan to ensure the industry has correctly trained staff. This includes the development of an industry common curriculum on key topics like AI awareness, VSS best practice, enhance the ability to use and share VSS information in a controlled and secure manner.

Enabling activities: Enhance current Learning & Development with Strategy and workforce planning, and map current and future skills needed. Create signature learning programs and use learning analytics to track engagement, completion and impact.

1.2 Change Management

Ability to plan and manage the industry change impact. It ensures that changes are adopted smoothly and deliver the intended benefits. Use change enablers like Change Champions, a communication strategy and leadership sponsors to support and sustain change initiatives.

Enabling activities: Enhance through existing processes like stakeholder engagements, communication, training and reinforcement. Support with active and visible exec sponsors and Change Champions. Create digital platforms for collaboration, feedback and tracking adoption with KPIs and lessons learned.

1.3 Resource Management

Ability to effectively allocate, monitor and manage resources to optimise VSS activities. Enhance the resourcing forecasting capability across the VSS model, use cases and incident impact.

Enabling activities: Enhance workforce planning based on demand and capacity. Create a competency tracking tool to maintain an up-to-date inventory of employee skills. Understand current and future capacity constraints and needs according to different use cases.

1.4 User-Friendly Experience

Ability to consistently design and deliver accessible and intuitive experiences for users of VSS management platforms. This is essential for driving engagement and satisfaction.

Enabling activities: Create a web-based interface, mobile access, providing clear and actionable alerts and simplified workflows for operators, including BTP staff.

2.1 Feedback and Evaluation

Ability to consult the public, gather comments, navigate press (positive and negative) and suggestions from customers and users. Then analyse and act to improve the experience with the railway. Essential capability for continuous improvement and accountability.

Enabling activities: Enhance channels for collecting input from employees, users and stakeholders. Enhance the tools and systems to gather and analyse the data. Create governance for avoiding bias and ensuring transparent reporting and accountability.

3.1 Roles and Responsibilities

Ability to clearly define, communicate and manage key roles and responsibilities across the industry organisations to ensure better collaboration. This will prevent overlap and duplication of work across the railway.

Enabling activities: Create an industry RACI to map responsibilities across processes and governance structures. Link roles and responsibilities to VSS Strategy objectives and KPIs. Create mechanisms to update roles as industry needs change.

3.2 Culture

Ability to embed shared values, behaviours and norms around safety and security that guide people across the railway to support strategic objectives, engagement and performance. Support the standardisation and tech adoption aspirations.

Enabling activities: Create a clear set of principles aligned with the VSS mission statement and Strategy. Define core values. Create culture diagnostics and maturity assessment for continuous improvement based on insights.

3.3 Ways of Working

Ability for the industry via the VSS Strategy to create a shared, effective and adaptive approach to collaboration, decision making and delivery.

Enabling activities: VSS Strategy supports the creation of an operating model and governance frameworks to provide a clear structure for decision making, accountability and team interaction.

2 Enabling high performance through capabilities

The ability to deliver strong, measurable results efficiently and consistently by using available resources.

KEY: Aspiration group Level 1 | Capability Level 2 | Priority Capabilities

4. BENEFIT DRIVEN DEPLOYMENT
- 4.1 Benefits Management
- 4.2 Programme Delivery

5. PERFORMANCE ENHANCEMENT
- 5.1 Governance
- 5.2 Assurance
- 5.3 Performance Definition
- 5.4 Performance Driven Improvement

6. PROACTIVITY
- 6.1 Risk Management

4.1 Benefits Management

Ability to identify, plan and realise the intended benefits of individual deployment with supporting business cases. This applies to renewals, enhancements with whole new CCTV systems or AI camera deployments. Ensure the value/cost is identified, delivered and sustained.

Enabling activities: Identify benefits and linking them to the strategic objectives and business case. Assigning benefit owners responsible for realisation. Create tracking and regular reviews to assess realisation and adjust plans.

4.2 Programme Delivery

Ability to have oversight of major VSS programmes to be carried out. The high-priority deployments should be captured in an industry overview.

Enabling activities: Enhance escalation paths and contingency planning with VSS Strategy governance for major programmes. Structure engagement plans for key stakeholders. Establish a major programme oversight across the industry for the delivery of the VSS Strategy.

5.1 Governance

Ability to establish and maintain effective practices and processes for decision-making. It ensures that strategic objectives are met, risks are mitigated, and resources are used effectively.

Enabling activities: Enhance VSS Strategy delivery roles, forums and decision-making bodies through RSSB and RDG. Create escalation paths and conflict resolution mechanisms. Continuous improvement and maturity assessment for capability building.

5.2 Assurance

Ability to verify that the VSS Strategy delivery programmes and initiatives are being executed effectively, ethically and in alignment with strategic objectives. This ensures that risks are managed and standards are met with intended outcomes.

Enabling activities: Create assurance framework and establish assurance roles for defined principles and processes. Integrate assurance with VSS strategy governance. Embed assurance into delivery and governance culture.

5.3 Performance Definition

Ability to define reliable, usable and measurable performance indicators that will track progress in achieving planned results against the policies, Strategy and objectives while supporting decision making.

Enabling activities: Enhance the VSS Strategy's qualitative and quantitative performance indicators. Continuously review and update performance definition to reflect changing needs and gathered feedback.

5.4 Performance Driven improvement

Ability for the industry to analyse and use VSS performance data and insights to continuously enhance its operations, services and strategic outcomes. This creates a proactive and data driven improvement system and culture.

Enabling activities: Conduct operational process review for improvement identification and enhance decision making using performance insights to guide prioritisation and resource allocation. Initiate process improvement initiatives and establish leaders championing data-informed improvements and embed improvement into the VSS Strategy delivery roles and responsibilities.

6.1 Risk Management

Ability to capture, report and monitor the risks that could impact the strategic objectives, operations or compliance of the VSS Strategy during delivery. It will enable the responsible parties to manage and mitigate the impacts on the railway. Risks should be accepted and managed with an appropriate plan of action.

Enabling activities: Enhance the existing risk management capability by integrating with the VSS Strategy governance and creating escalation paths. Implement risk mitigation strategies and control measures with regular reporting to leadership. Embed risk awareness into decision making.

3 From compliance to public confidence

The ability to commit to being transparent, responsible and responsive to the people it serves or affects.

KEY: Aspiration group Level 1 | Capability Level 2 | Priority Capabilities

7. REGULATION
- 7.1 Regulatory Change Management
- 7.2 Personal Data Protection
- 7.3 Legal Compliance

8. SECURITY & COMPLIANCE
- 8.1 System Security

9. TRANSPARENCY
- 9.1 Communication
- 9.2 Knowledge Management

10. ETHICS
- 10.1 Ethical Awareness
- 10.2 Ethical Governance

7.1 Regulatory Change Management

Ability to identify, assess, respond, and implement regulations and compliance standards changes around cameras and VSS. Continuously tracking new or updated regulations from relevant authorities and evaluating the impact on the railway. This is particularly important as technology evolves rapidly.

Enabling activities: Updating internal policies, procedures, and controls to align with regulatory changes. Learning from past regulatory changes to improve future responsiveness, Horizon scanning for upcoming changes.

7.2 Personal data protection

Ability to safeguard individuals' personal information through its lifecycle - collection, storage, use, sharing and disposal while complying with legal and ethical standards like UK GDPR, Data Protection Act 2018 and other relevant regulations.

Enabling activities: Enhance monitoring and auditing capabilities by conducting regular data privacy audits and risks assessments. Ensure VSS Strategy initiatives comply with personal data protection. Embed DPIAs in any expansion of access rights. Review cross-organisation data sharing agreements enhancing and promoting a culture of privacy and accountability by sharing policies and best practices.

7.3 Legal Compliance

Ability to understand, implement and adhere to laws, regulations and internal policies that apply to the railway's operations.

Enabling activities: Enhance ongoing compliance checks, internal audits, and control testing. Create a robust compliance framework and governance. Learning from past regulatory changes to improve future responsiveness.

8.1 System Security

Ability for the VSS network to protect itself against threats, detect vulnerabilities and respond to security incidents. Cybersecurity capability will evolve to ensure that the service and operational efficiencies, which can result from a smarter VSS are design with strong in security and ethics.

Enabling activities: Create strong security measures such as encryption, firewalls, and regular updates. Ensure compliance with data protection standards. Ensure only authorised users can access the system – Organisations need to have a mature cybersecurity function and cybersecurity standards.

9.1 Communication

Ability to effectively exchange information with the railway ecosystem. This includes customers, partners, suppliers, regulators, media and the general public. Using different channels, like digital, to share Information and engage with a variety of stakeholders. With a clear value proposition and key messages, this reduces misunderstandings and errors while contributing to a common culture around safety.

Enabling activities: Enhance internal and external communication with VSS Strategy delivery outcome progress. Assess current communication tools and practices to identify gaps and effectiveness.

9.2 Knowledge Management

Ability to effectively capture, share, use and retain knowledge to improve performance, innovation and decision making. This ensures that valuable information and expertise are not lost and are accessible to the right people at the right time.

Enabling activities: Enhancing collaboration through communities of practice, forums and social platforms. Encouraging industry exchange with a knowledge management strategy. Tracking usage, contributions and impact of knowledge assets like the Strategy document. Assess the feasibility of a centralised knowledge hub or portal.

10.1 Ethical Awareness

Ability to analyse case studies or ethical dilemmas and encourage open dialogue to recognise, understand and respond to ethical issues thoughtfully and responsibly.

Enabling activities: Enhancing training and creating ethical decision-making toolkits for employees, leaders and stakeholders with scenario-based learning to build decision-making skills. Embedding ethics into policies, performance management and strategic planning.

10.2 Ethical Governance

Ability to embed ethical principles into the VSS Strategy governance structure, decision-making processes, and leadership behaviours. Notably by building ethically robust AI systems and gaining trust. This will guide the railway to act with integrity, fairness and accountability.

Enabling activities: Establish clear roles and responsibilities for ethical risk management. Embed ethical considerations in strategic and operational decisions. Integrate ethics into training. Move to AI systems that are ethical by design.

4 Bridging gaps with greater accessibility & connectivity

Ensuring that people, systems and resources can easily access and connect with each other.

KEY: Aspiration group Level 1 | Capability Level 2 | Priority Capabilities

11. CONNECTIVITY

- 11.1 Connected System
- 11.2 Image Usability
- 11.3 Environmental Efficiency

12. ACCESSIBILITY

- 12.1 System Availability
- 12.2 System Adaptability
- 12.3 Timely Accessibility

11.1 Connected System

Ability to design, integrate and manage systems that are data-driven and seamlessly connected across platforms and stakeholders. Connect priority stations to BTP. This is important to enable real-time insights, collaboration and agility across the network.

Enabling activities: VSS must be remotely viewable in chosen locations, which may include NOCs, ROCs, TOC Control Centres and in specified sites for vital industry stakeholders, including BTP. Create access to authorised users for real-time and recorded footage for observation and control.

11.2 Image Usability

Ability to ensure that images used across digital platforms are accessible, effective, and user-friendly. A core element of the VSS Strategy, this will allow users to convey information and enhance user experience across the railway. Image quality must be sufficient for the use case with DORI Guidance (Detection, Observation, Recognition, and Identification) used to guide site design.

Enabling activities: Comply with the DORI framework (Detection, Observation, Recognition, and Identification). Create an intuitive and accessible user interface and experience across devices. Images and events must be visually distinguishable under variable lighting, weather, and environmental conditions (e.g. rain) to support situational awareness and enable timely decisions.

11.3 Environmental Efficiency

Ability for the rail industry to minimise its environmental impact while optimising resources across operations and services. This helps with sustainability goals and regulatory compliance. The railway is in an Eco-Digital era where there is a dual transition to a sustainable and digital economy. Sustainability efforts are supported by the shift toward digital first.

Enabling activities: Align VSS Strategy and strategic objectives with industry sustainability strategy and roadmap to minimise energy use and asset base without compromising performance. Create training to upskill employees in eco-efficient practices.

12.1 System Availability

Ability to ensure that VSS systems are consistently operational, accessible and performant – especially during peak demand or unexpected disruptions. A key aspect of the VSS Strategy is to realise the industry vision.

Enabling activities: Enhance the resilience of the system, including back-up for critical functions, and alerts provided in the event of a system failure. The system should continuously monitor system performance, provide remote self-diagnostics and raise alerts to reduce operational costs and carbon footprint.

12.2 System Adaptability

Ability to modify, scale, and evolve its systems, technological or operational, in response to changing internal and external conditions. Essential for the VSS resilience, innovation and long-term efficiency.

Enabling activities: Create an interface with existing 'control' systems (e.g., command and control tools, legacy cameras, third-party analytics) with minimal retraining or business disruption. Must enable integration with third-party systems and future technologies, for example by using open APIs (Application Programming Interface) and ONVIF (Open Network Video Interface Forum) compliance. Should enable a repeatable 'GBR-ready' architecture, able to grow and adapt to future needs, without vendor lock-in.

12.3 Timely Accessibility

Real-time and recorded footage must be available to authorised users with minimal delay, regardless of location. Must support role-based prioritisation (e.g. BTP access to critical footage during incidents). Ability to detect unauthorised access and system anomalies instantly.

Enabling activities: Role-based prioritisation is a critical development for the realisation of timely accessibility. Instant detection of unauthorised access and system anomalies. Then, with the support of AI, provide real-time footage access and access without delay.

5 From silos to systems with Technology Integration

The ability to effectively incorporating digital tools, systems, and innovations to enhance performance.

KEY: Aspiration group Level 1 | Capability Level 2 | Priority Capabilities

13. TECHNOLOGY
- 13.1 AI, ML & Computer Vision
- 13.2 Future Tech, Drones & Robotics
- 13.3 Tech Architecture

14. DIGITAL FIRST
- 14.1 Transition From Analogue To IP Cameras

15. STANDARDISATION
- 15.1 Vendor Rationalisation
- 15.2 Format Compatibility

13.1 AI, ML & Computer Vision

Ability to undertake AI prioritisation and risk assessments. Ensure that staff are consulted about AI solution design and upskilled in using any AI systems. Create the ability to design and use AI in the context of VSS to improve efficiency and decision-making. The use of AI is to be regulated and in line with the compliance and ethical governance for better use.

Enabling activities: Undertaking AI risk assessments. The hub and spoke model is designed initially as a Network Rail specific model that allows for engagement with the wider industry. However, this model also provides a path to evolve and be adopted across the industry in a post-GBR landscape.

13.2 Future Tech, Drones and Robotics

Ability to use drones and robotics for manual flight operations or automated inspections and monitoring of remote or hazardous areas. This will allow operators to enhance incident response and assessment with faster and more comprehensive data collection.

Enabling activities: Create future tech capability for analytics of real-time detection of hazards, providing alerts for human response or through connection to other systems (more details in the Deep Dive (Appendices) section).

13.3 Environmental Efficiency

Ability to set the skills, processes, tools and governance structures that will enable the industry to design, implement, and evolve its technology landscape in alignment with the Strategy objectives. Critical to the industry's digital transformation, the Tech architecture will define a cloud or on-prem solution for the storage of footage. The Tech Architecture capability looks at the ability to create effective retention schedules and methods for this new VSS footage.

Enabling activities: Enhance the technical architecture to improve agility and scalability with cloud or on-prem solutions, reduce technical debt and enhance security and compliance (more details on the DORI Framework in the Deep Dive (Appendices) section).

14.1 Transition from Analogue to IP Cameras

Ability to switch from legacy analogue systems reaching the end of life to IP cameras and follow the DORI framework. This capability covers the ability to evaluate the network capacity, storage needs, and ensure cybersecurity measures are in place for the software integration. The DORI framework provides a structure for defining camera performance expectations based on intended use. Adopting this model helps to ensure a consistent and purposeful approach across the rail estate.

Enabling activities: This transition will allow operators to have the image quality that will be sufficient for the use cases with DORI guidance used to guide site design (more details in 2.2.2).

15.1 Vendor Rationalisation

Ability to manage the contracts of vendors, ensuring good quality and timely delivery of goods & services. Liaising with Vendor Development and Supplier Relationship Management. Enhance the ability to improve efficiency, reduce costs, and strengthen supplier relationships across the railway.

Enabling activities: Develop and execute a rationalisation plan by prioritising categories and vendors, and ensure continuity of service during transitions. Continuously review vendor landscape and adjust Strategy based on business changes.

15.2 Format Compatibility

Ability for the systems to work seamlessly across different data formats, file types or standards.

Enabling activities: Enhance commonly used video standards (e.g., MP4, H.265) and integrate with evidence management tools, archival platforms, and analytical software without requiring conversion. Must be compatible with other 'protection' systems such as perimeter measurement systems, obstacle detection and passenger-facing systems such as PAVA.

Accelerating impact with the prioritised capability deployments

This roadmap outlines key capability deployments designed to enhance railway operations, governance, and public accountability. It highlights strategic priorities across people, performance, and technology to accelerate impact, starting from the strategy implementation and the right governance being put in place.

Phase 1 – Indicative timeline 2026-2027

People Focus

Industry RACI: Identify the process and decisions that need role clarity. Then identify the teams involved for the relevant tasks. Review and agree on the RACI matrix for the VSS deployment.

Resource Management: Enhance the resourcing and resource forecasting capability across the VSS model, use cases, and incident impact. Define how demand is captured and resource allocated with appropriate governance.

Change Management: Enhancement through existing processes like stakeholder engagements, communication, training and reinforcement. Support with active and visible exec sponsors and Change Champions.

Ways of working: VSS Strategy support the creation of an operating model and governance frameworks to provide a clear structure for decision making, accountability and team interaction.

Learning and adoption with signature program: Enhance current Learning & Development with strategy and workforce planning, map current and future skills needed, and create a signature learning program on key topics like AI awareness, VSS best practice, the ability to use and share VSS information in a controlled and secure manner.

Digital Platforms: Create digital platforms for collaboration, feedback and tracking adoption with KPIs and lessons learned.

User-friendly experience: Create a web-based interface, mobile access, and provide clear and actionable alerts and simplified workflows for operators, including BTP staff.

Rail Performance

Assign benefit owners for benefit management: Develop supporting business cases for VSS deployment. This applies to renewals, enhancements with whole new CCTV systems or AI camera deployments. Ensure the value/cost is identified, delivered and sustained.

Footage access primacy: Create a policy/process which agrees on the primacy of footage access between NR, BTP and the TOCs when an incident happens.

Governance with effective risk management: Enhances VSS Strategy delivery roles, forums and decision-making bodies through RSSB and RDG. Create escalation paths and conflict resolution mechanisms. Embed risk awareness into decision-making and encourage proactive risk escalation with communication while building a risk-conscious culture.

Accessibility and Connectivity

Mature cyber security organisation: Enhance security measures such as encryption, firewalls, and regular updates. Ensure compliance with data protection standards. Ensure only authorised users can access the system – organisations need to have a mature cybersecurity framework and cybersecurity policies.

Creating a security policy or process for viewing footage in public spaces: Remote footage will be accessible anytime, anywhere, and this may usually be accessed in a control centre. However, if any footage is reviewed in public places, there must be guidance and policies to manage this.

Enhanced communication: Effectively exchange information with the railway ecosystem. Using different channels, like digital, to share information and engage with a variety of stakeholders. This includes customers, partners, suppliers, regulators, media and the general public. Clear value proposition and key messages. This reduces misunderstandings and errors while contributing to a common culture around safety.

Accountability to the Public

Connected System: VSS must be remotely viewable in chosen locations, which may include NOCs, ROCs, TOC Control Centres and in specified sites for vital industry stakeholders, including BTP. Create access to authorised users for real-time and recorded footage for observation and control.

Retention schedules review for VSS stored footage: The current retention schedule needs to be reviewed for storing data for different use cases, i.e. for training AI models, infrastructure monitoring or criminal investigations.

Timely Accessibility: Role-based prioritisation is a critical development for the realisation of timely accessibility. Then, instant detection of unauthorised access and system anomalies. Then, with the support of AI, provide real-time footage access and access without delay.

Technology Interaction

DORI Framework for IP transition: The DORI framework provides a structure for defining the camera performance expectations based on intended use. Adopting this model helps to ensure a consistent and purposeful approach across the rail estate. This transition will allow operators to have the image quality that will be sufficient for the use cases with DORI guidance used to guide site design (more details in the Tech Transformation section).

Undertake AI Risk Assessments: Helps identify AI Prioritisation, and risks to be managed in development and delivery.

Tech Architecture: Enhance the technical architecture to improve agility and scalability with cloud or on-prem solutions, reduce technical debt and enhance security and compliance (more details in Tech section).

AI, ML & Computer Vision: The hub and spoke model is designed initially as a Network Rail-specific model that allows for engagement with the wider industry. However, this model also provides a path to evolve and be adopted across the industry in a post-GBR landscape.

2.2 TECHNOLOGY TRANSFORMATION

SECTION TAKEAWAYS:

The Technical Strategy has been developed from the inputs of all major rail stakeholders.

The technical strategy translates user requirements into practical recommendations that address key challenges in quality, coverage, connectivity, and security, guiding the industry on how to deliver consistent, high-performing VSS solutions across the rail network.

Technical Strategy on a page

This one-page technical strategy summary serves as an overview, distilling the key takeaways and strategic priorities from each section of the broader technical architecture.

1 User and Technical Requirements

User 'Functional' Requirements:

I need video images that are accessible, available, usable and secure.

System 'Technical' requirements:

VSS must be connected from the edge to the user. It must detect hazards, alert users to improve human responses and reduce risk. It must be secure, resilient, and scalable.

2 Quality Improvements

Selecting the right camera is key—not only for achieving high image quality, but also for enabling better connectivity, stronger security, and cloud readiness across the system.

3 Coverage Improvements

In VSS System planning and assessment, the DORI standard (Detection, Observation, Recognition, Identification) provides a structured framework for defining camera performance expectations based on intended use. Adopting this model helps to ensure a consistent and purposeful approach across the rail estate.

4 Connectivity

1; Connectivity:
Use IP-enabled cameras. Choose a network based on location and use case.

2; Cybersecurity:
IEC-compliant design on ZT principles and with security controls.

3; Integration and Control Room Functionality:
Cloud-Based Security Integration Layer (SIL) integrates across layers and provides a universal interface.

Distributed model of existing rooms plus remote, authorised access.

The proposed technical architecture addresses 3 key themes to ensure the industry benefits from higher quality, broader, and faster access to footage.

To deliver the benefits needed, the technology transformation section addresses key challenges around: **quality, coverage, and connectivity** of the rail VSS estate.

Quality

High-definition, standards-compliant cameras and analytics-ready infrastructure ensures all video streams are clear, reliable, and suitable for evidential use, supporting operational and safety outcomes.

Coverage

Camera placement and system design guided by the DORI (Detection, Observation, Recognition, Identification) standard, ensure that every critical location achieves the right level of visual detail for its operational and safety needs.

Connectivity

Connectivity:

Deploying resilient, high-bandwidth network infrastructure as a foundation for real-time access to VSS footage, enabling faster diagnostics, monitoring, and cloud integration across the estate.

Cybersecurity:

Once connected, the system's cyber threat profile changes. Controlled access for stakeholders to encrypted streams is needed to securely provide the enhanced situational awareness required.

Integration:

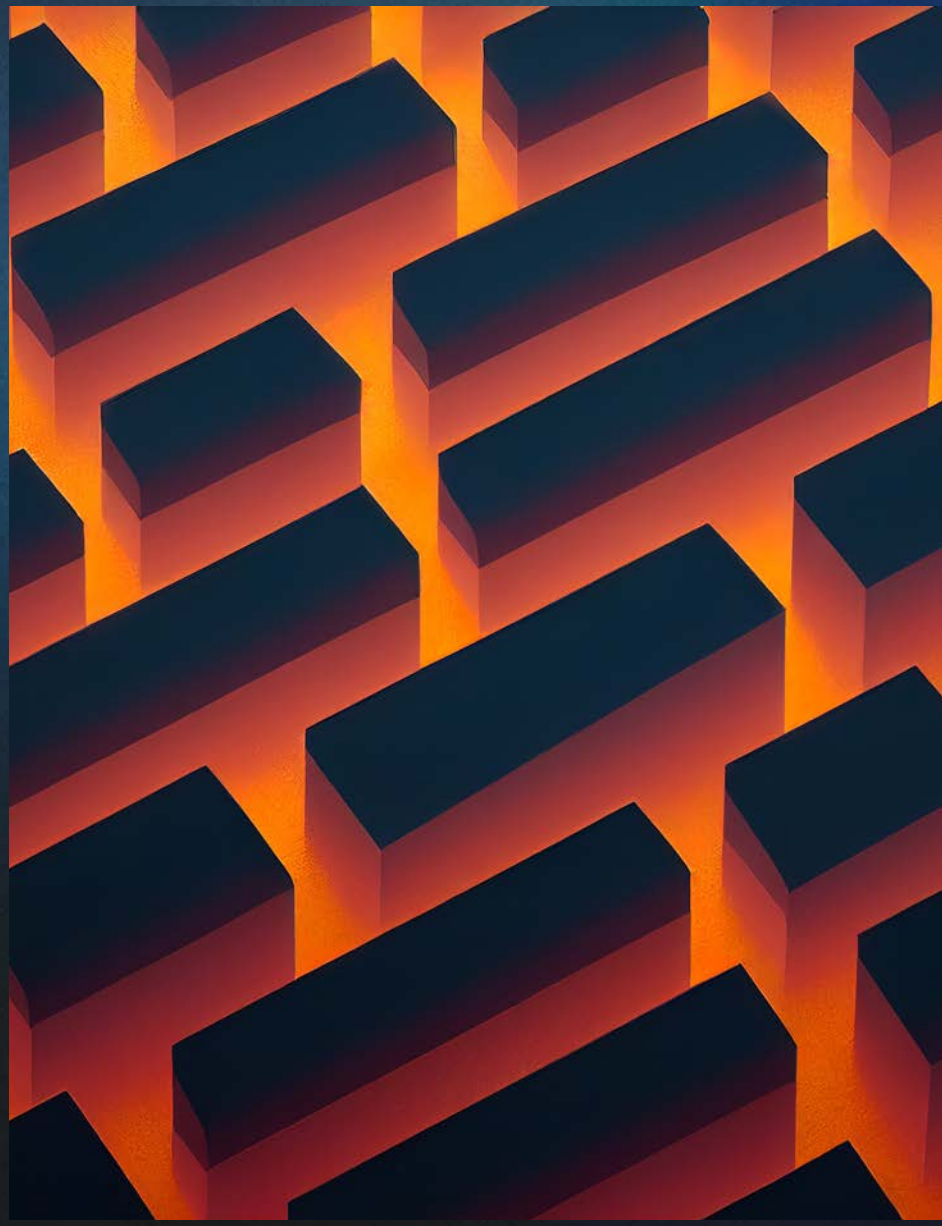
Implementing a cloud-based System Integration Layer (SIL) that consolidates live and recorded video streams from across the estate, enabling control rooms and authorised users to access, assess, and respond to incidents in real time for superior hazard management and incident containment.

2.2.1

VSS FUNCTIONAL AND TECHNICAL REQUIREMENTS

SECTION TAKEAWAYS:

Depending on the specific use case, these functional and technical requirements must be included in the specification and procurement of all future VSS systems and sub-systems.



Users' requirements for VSS are broken down into Functional Requirements that should be used to define future VSS systems

Any system, regardless of its potential, will only be widely adopted and maintained if it meets user requirements.

These Functional Requirements must be used to specify future VSS systems to ensure strategic compliance.

Quality

I need video images that are clear and usable

Must: Deliver an intuitive, accessible interface across all devices.

Must: Ensure images and events remain visually clear in all lighting, weather, and environments to support awareness and timely decisions.

Coverage

I need optimal coverage for security and efficiency

Must: Eliminate blind spots in all critical areas.

Must: Minimise overlap and avoid redundant cameras.

Connectivity

I need timely access to footage

Must: Provide real-time and recorded footage to authorised users with minimal delay, anywhere.

Must: Support role-based prioritisation of footage (e.g., BTP access during incidents).

Must: Detect and report events and hazards instantly.

I need systems to be compatible

Must: Be compatible with other protection systems (e.g., perimeter measurement, obstacle detection, PAVA).

I need VSS systems to be built on existing technology

Must: Interface with existing control systems (e.g., command tools, legacy cameras, third-party analytics) with minimal retraining or disruption.

Must: Enable integration with third-party systems and future tech via open APIs and ONVIF compliance.

I need the VSS system to be resilient

Must: Ensure system resilience with backup for critical functions and alerts on failure.

My VSS system must be secure

Must: Implement strong security measures (e.g., encryption, firewalls, regular updates).

Must: Ensure compliance with data protection standards.

Must: Ensure only authorised users can access the system.

To see the user requirements and how these functional requirements were derived, see Appendix 3.1.1.
To see further detailed functional requirements, see Appendix 3.1.1.

The Technical Requirements will deliver the unified, scalable and resilient industry-wide VSS capability required by the Strategy

These Technical Requirements must be used to specify future VSS systems to ensure strategic compliance.

They have been agreed upon by all stakeholders and combined with the Functional Requirements to deliver the Industry Vision.

Quality

Coverage

Connectivity

Usable and Protected Image Data

Must: Apply DORI guidance for image quality and coverage.

Must: Protect data with AES-256 encryption, secured hardware, access controls, GDPR compliance, and data retention standards.

Resilient Connectivity

Must: Ensure network connectivity provides high levels of reliability, availability and maintainability.

Provide Secure Access

Must: Use encrypted streams (e.g., VPN/AES-256) with secured access, including MFA, SSO, role-based access control, session timeout, and audit logs.

Zero Trust and Cybersecurity Built In

Must: Apply Zero Trust Architecture principles.

Integrated Systems and User Experience

Must: Integrate cameras, storage, and user interfaces with open APIs, ONVIF compliance, and common data models (JSON, XML).

Connected System

Must: Allow remote viewing from designated locations (e.g., NOC, TOC, stakeholder sites).

Must: Provide authorised users with real-time and recorded footage for observation and control.

Other capabilities

Detect Hazards, Incursions and Anomalies

Must: Where use case requires, provide real-time analytics to detect hazards and trigger alerts for human response or system integration (e.g., Voice Alarm).

Facilitate Future Scalability

Must: Be vendor-agnostic and cloud-ready, supporting local storage, analytics tools, and AI services.

Resilient System

Must: Meet targets, which could be delivered through uninterruptible power supply, failover mechanisms, disaster recovery, and continuous uptime monitoring.

User-Friendly Experience

Must: Include a web interface and mobile access with clear alerts and simplified workflows.

Compliant System Design

Must: Comply with stakeholder standards, national legislation, and relevant CCTV regulations for operation and monitoring in public spaces.

To see the user requirements and how these technical requirements were derived, see Appendix 3.1.1.
To see further detailed technical requirements, see Appendix 3.1.1.

2.2.2

VSS STRATEGIC PILLARS

SECTION TAKEAWAYS:

Focusing on quality, connectivity & security, and coverage, these VSS solution pillars provide a structured approach that ensures reliable, secure, and comprehensive visual monitoring, enabling industry-wide benefits such as improved safety, operational performance, and a shared pathway for future VSS development.

2.2.2 VSS STRATEGIC PILLARS A QUALITY

Selecting the right camera technology not only enhances image quality but also strengthens connectivity, security, and cloud readiness across the system.

Procurement Guidance for Camera & Video Systems:

For asset owners (renewals and new purchases):

When renewing assets, purchasing new cameras or video systems, asset owners must ensure that equipment is future-proof, secure, and aligned with the wider VSS Strategy. The table acts as a checklist, setting out the minimum capabilities required from suppliers.

Using this guidance avoids costly retrofits and ensures systems can integrate smoothly with wider rail and partner environments.

Good practice additions:

- Secure watermarking or export options for evidential use.
- Compatibility with Cloud-Based SIL and wider operational systems.
- Open APIs for integration with third-party analytics and applications.

Minimum Capabilities

● Mandatory ● Preferred

Category	Requirement
● Video Quality & Compression	Support for H.264 and H.265 (HEVC) to balance quality with bandwidth and storage efficiency.
● Standards & Interoperability	ONVIF compliant (Profiles S/G/T) to ensure compatibility with multiple platforms.
● Connectivity	Connected to local VSS and connectable through Cloud-Based SIL to cloud / Data Centre storage.
● Security	Encryption for data in transit and at rest; secure firmware and patching.
● Access Control	RBAC, audit logging, federated authentication.
● Cloud Readiness	Hybrid on-premise/ cloud compatible.
● Edge Analytics	Edge analytics, or readiness, for specific use cases.
● Resilience	Local storage/buffering, UPS or batter-backup options.
● Scalability	License/performance model that supports easy expansion to other sites.
● Audit & Compliance	Logs user access, playback, and exports.
● Cybersecurity	Vendor processes aligned to Cyber Essentials Plus / ISO 27001 and ZT principles deployed.

Adopting the DORI standard not only improves image quality but also ensures comprehensive coverage tailored to key operational requirements

In VSS System planning and assessment, the DORI standard (Detection, Observation, Recognition, Identification) provides a structured framework for defining camera performance expectations based on intended use. Adopting this model helps to ensure a consistent and purposeful approach across the rail estate.

By assigning a DORI level to each surveillance zone, asset owners and planners can identify coverage gaps, avoid overlaps, and ensure the right level of monitoring is applied across different operational areas. This enables efficient use of cameras while maintaining visibility where it matters most.

DORI example within the rail context: Trespassing at a platform end.

Step 1: The engineer identifies the surveillance zone, e.g. a platform boundary.

Step 2: They assign the 'Detection' DORI level to ensure any movement or unauthorised presence is captured by analytics (e.g. line-crossing, loitering).

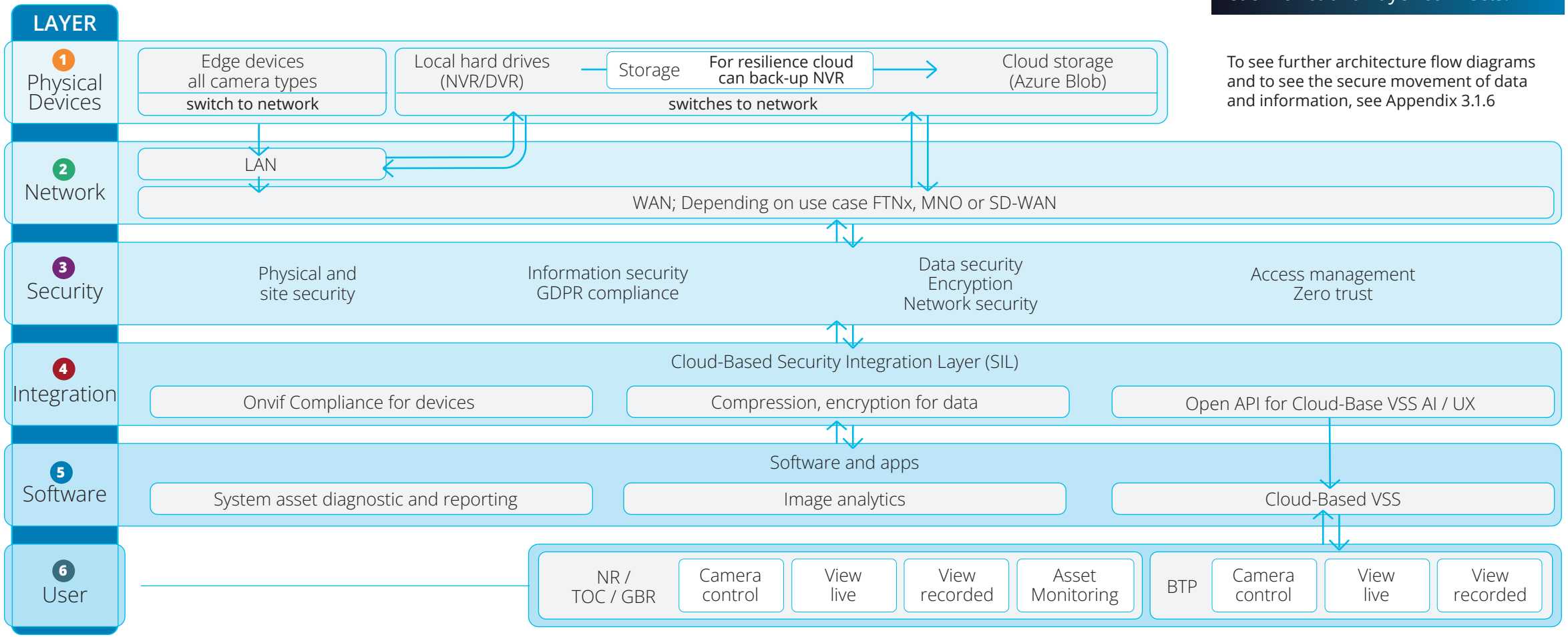
Step 3: For incident response and evidence, they verify if adjacent cameras deliver 'Recognition' or 'Identification' level footage, ensuring faces, clothing, or actions are clearly visible.

Step 4: If gaps appear (e.g. insufficient lighting or resolution), they adjust the lens type, angle or add supplementary coverage to achieve the target DORI level.

DORI Level	Example Use Case	Typical Location	Quality Role	Coverage Role
Detection	**Intruder presence, people counting** • Line-crossing or intrusion analytics • Thermal imaging for presence detection • Low-resolution fixed wide-angle camera	Car parks, perimeters, open platforms.	Image quality sufficient to confirm motion or presence (e.g. identifying that someone or something has entered a restricted zone).	Wide area awareness, entry point monitoring.
Observation	**Incident context, situational awareness** • People counting or crowd monitoring • Behavioural analytics (e.g. loitering, flow direction) • HD wide-angle or dome camera with moderate zoom	Ticket halls, corridors, entrances.	Moderate detail to understand what's happening, e.g. behaviour, movement direction or crowd flow.	Event understanding, people flow monitoring.
Recognition	**Known subject verification, behaviour tracking** • Appearance tracking, subject re-ID • Cross-camera correlation via attributes • Full HD PTZ or high-zoom camera with good low-light performance	Access gates, secure entrances.	Clear enough to tell who the person is from previously known subjects or to match against another camera view.	Focused area surveillance, watchlist matching.
Identification	**Evidential facial or number plate clarity** • Facial recognition or ANPR (number plate) capture • High frame-rate, high-resolution analytics for evidential review • 4K or multi-sensor camera with controlled lighting	Gate lines, custody areas, control zones.	Evidential quality facial clarity or number plate readable for investigation and prosecution.	Critical zone coverage for legal evidence.

The strategy connects assets to the network and securely integrates them into a cloud-based VSS, so users can access footage from control rooms or remotely.

This architecture should form the basis of all VSS systems. The VSS architecture shows the proposed **logical system structure,** including the different components and how each functional layer connects.



To see further architecture flow diagrams and to see the secure movement of data and information, see Appendix 3.1.6

The Cloud plays an important role in the future VSS strategy, not as a replacement for existing on-site storage, but as an enabler that supports secure access, collaboration and advanced functions across the railway.

Why use the cloud?

Local edge systems remain the backbone for day-to-day recording, while the Cloud provides the tools and scale to deliver services that individual sites cannot achieve alone.

Accessibility: Authorised users from BTP, Network Rail, and TOCs can connect securely from anywhere, without needing local links into every site.

Security: Avoids manual workarounds and ensures consistent audit controls.

Resilience: Cloud services are hosted in highly available data centres, reducing the risk of outages.

Scalability: Supports growth in analytics and system functions without heavy local infrastructure.

Cost: Lower costs due to local systems keeping recordings; Cloud is only used for advanced services and selective datasets.

Innovation: Enables advanced AI and cross-railway collaboration that is harder to run at every site.

How does it work and tie into the Cloud-Based System Integration Layer (SIL)?

1. Video remains at the edge; day-to-day video recording stays on station or site servers, not sent continuously to the Cloud.
2. When authorised users request footage, the cloud platform automatically brokers a secure connection to the relevant edge device, retrieves only the approved video segment, and transfers it through an encrypted and fully audited process.
3. Controlled access authorised users log in through a secure portal with SSO/MFA to view or request approved content.
4. Selective use of only datasets prepared for training, education, or specific case needs is under control if required.
5. The Cloud forms part of the Security Integration Layer, where data, analytics, and access controls are brought together.
6. APIs and AI functions in the Cloud provide a single, standard way to connect different systems (video, access control, incident management).

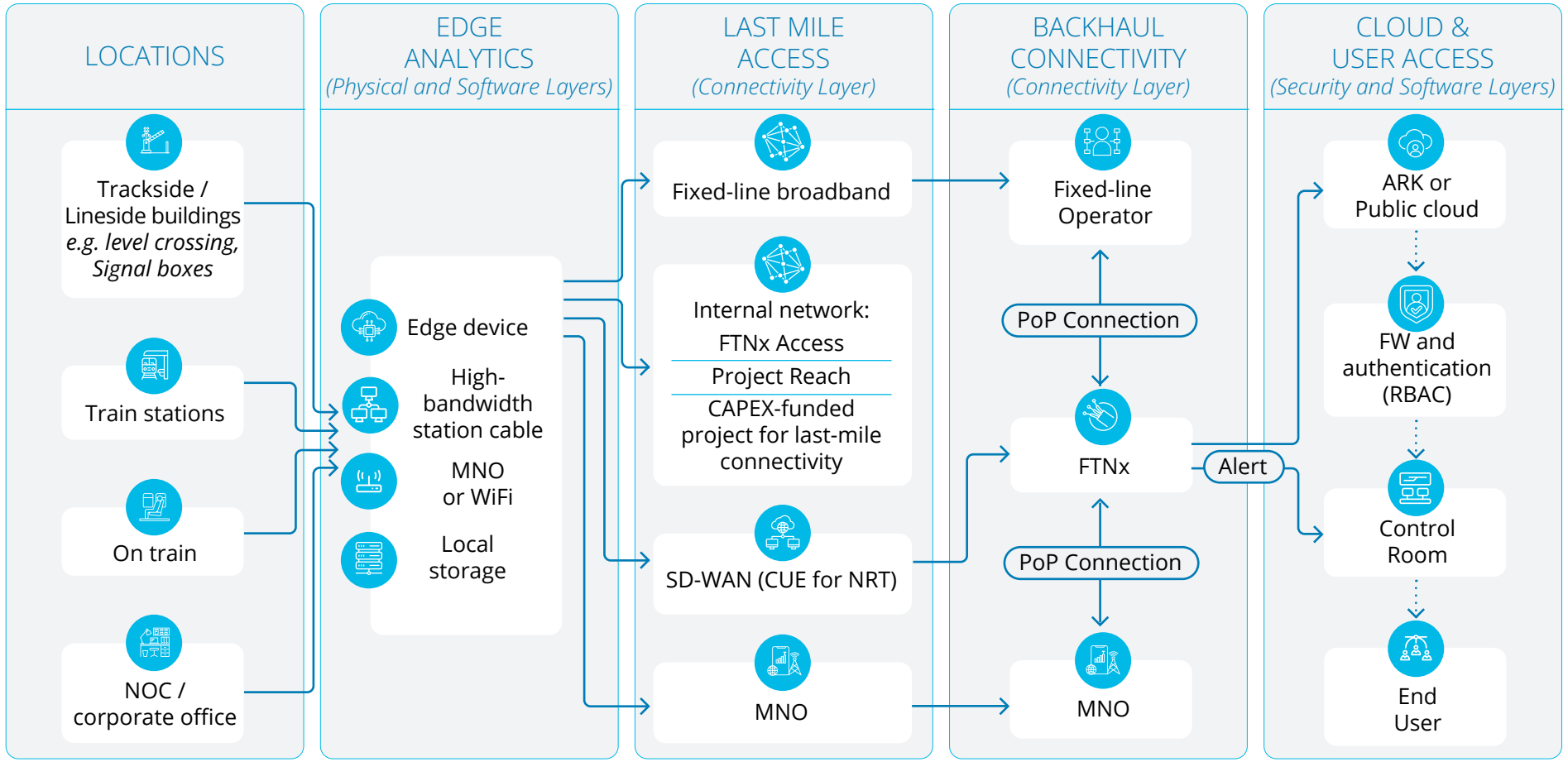
What the cloud **does not** do:

It does not store every second of video from every camera on the network.

It does not replace local recording, which remains the primary storage for compliance and investigation.

It does not give uncontrolled access; strict permissions and audit logs are applied.

The connectivity model helps select the best network options for VSS, making footage accessible wherever it's needed across the rail network.



The connectivity of systems is central to achieving strategic compliance. This connectivity model should be followed.

The current VSS estate strongly reflects the **proliferation of local applications with only local ambition.** These meet the minimum needs for each individual site, but the accessible advantages of aggregating the data and imagery are missed.

The model here shows the **recommended connectivity architecture:**

↑ Secure data flow between systems (e.g. edge to cloud, cloud to DR).

↕ Secure bi-directional data commands and heartbeat signals.

To see further detailed connectivity options and their cost/complexity, see Appendix 3.1.2

Embedding cybersecurity into VSS not only protects data but also builds trust and ensures compliance across the system.

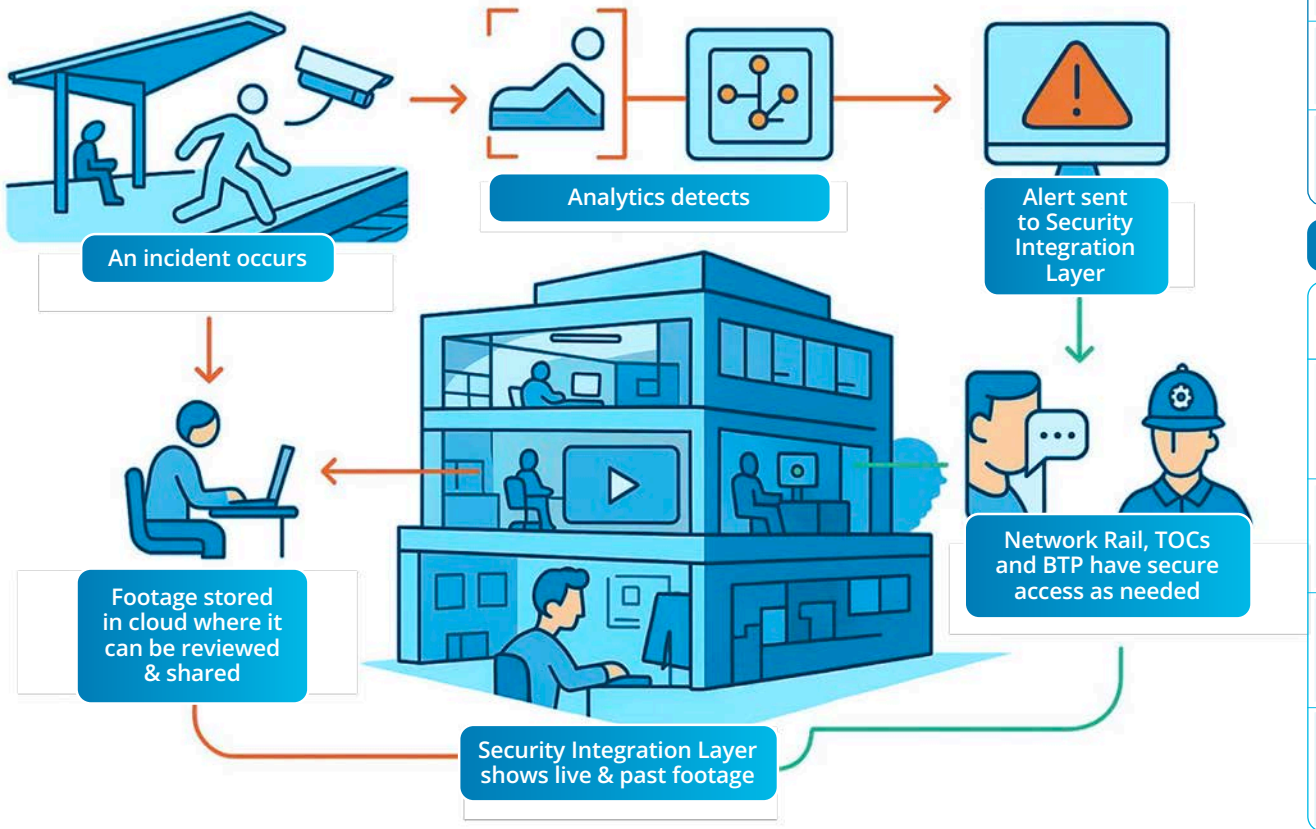
Cyber controls must be specified for the future VSS system. Below is a sample of Microsoft, Zscaler and other controls used across the industry. They can be modified to support vendor-agnostic implementations in future architecture designs.

Cyber Security	Cyber Security Control	Illustrative Controls for VSS Using Existing Technologies	Zero Trust Alignment
Provide Secure Access	**Role (+Organisation) Based Access Control for Video Systems (RBAC)**	RBAC via Entra ID and Zscaler ZPA to control access to video feeds and remote consoles based on user attributes.	Context-aware access control
	Policy Enforcement for Camera Systems	Group Policy and Intune to enforce Windows NVR/VSS security baselines; Linux/embedded cameras use custom scripts and Zscaler for network policy.	Enforce least privilege and device trust
	Enable MFA for all CCTV access	MFA via Entra ID, Intune, or Authenticator for all endpoints and VSS storage; Zscaler ZPA enforces secure, role-based access.	Verify explicitly and assume breach
Strong Security Measures *(Video Footage Security)*	**Encryption of Video Storage**	BitLocker (Windows), LUKS (Linux), or vendor-native encryption enforced for NVRs with minimum AES-256; Azure Storage Encryption used for cloud video archives.	Data protection at rest
	Patch Management for Video Systems	Intune, Azure Update Management, or vendor tools used for firmware/OS updates on cameras, NVRs, VSS servers; integrated with change management.	Maintain secure and updated systems
	Secure Data flow	Use TLS 1.2 or higher to ensure secure data transmission between cameras, NVRs, servers, etc.	Data Protection in motion
	Connectivity and Network Security	Camera →Security Integration Layer Server: Enforced via NSG rules and IDS monitoring. Cloud-Based SIL →Azure Services: Secured via Zscaler and Azure Firewall. Data Flow →Cloud Storage: Encrypted and monitored via DLP and Sentinel.	Defence by depth and Assume breach
Monitor VSS health	**Cloud-Based SIL User Activity Monitoring**	Leverage Microsoft Defender for Cloud Apps, Splunk, CYJAX, Dark Trace etc. to track user sessions, access patterns, and anomalies for cyber threats.	Continuous Monitoring
Compliant System Design *(Data Protection Compliance)*	**GDPR Compliance controls**	Data minimisation - Configure Video Systems to only record necessary areas and avoid capturing excessive or irrelevant footage (e.g., private property).	GDPR
	Retention and Deletion Policies	Define common retention periods (typically 31 days unless required for investigation). Ensure Data Protection Impact Assessments (DPIAs) are completed for all deployments.	Data Privacy compliance
	Network Security Compliance (IEC 62443)	Implement network segmentation using IEC 62443's zones and conduits model. Group assets with similar security requirements into defined zones and manage inter-zone comms.	Enforce least privilege and device trust

To see further detailed cybersecurity requirements see Appendix 3.1.3

Users will have access to live and recorded footage from all connected assets across the VSS estate, with data security built in

Once the integration layer is established, the information journey from incident to user is clear, as shown for the Trespass and Vandalism use cases



Vandalism Detection

Stage	Action	Impact
Detection	Analytics detect unusual behaviour near high-risk areas.	Suspicious behaviour alert sent to the Cloud-Based SIL interface.
Event Correlation	Live alerts are received with linked video, sensor input.	Operators receive automated alerts and visuals immediately.
Response Coordination	Operators inform site security or dispatch BTP with incident context and location.	Real-time access to video and timeline playback supports quick escalation.
Evidence Capture & Follow-up	Footage is exported and securely stored as evidence.	Cloud-Based SIL simplifies audit, storage tagging, and footage transfer.

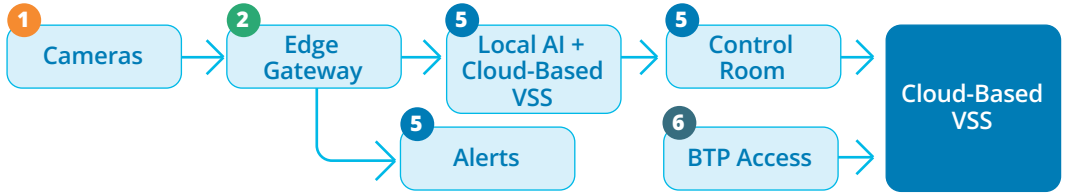
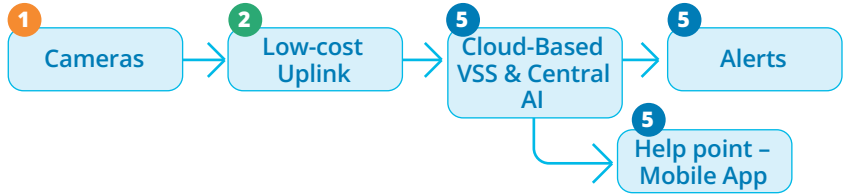
Trespass Detection and Response

Stage	Action	Impact
Detection	AI analytics on edge devices *(e.g. camera zones or trackside sensors)* detect motion in restricted areas.	Data flows securely to VSS -> Cloud-Based SIL for real-time alert generation.
Event Correlation	Cloud-Based SIL links the trespass alert with associated CCTV, access logs, or past incidents	Control ops understand context in real time *(e.g. area, time, operator [Local / Cloud] alerts).*
Response Coordination	Control room operator alerts on-site personnel and informs BTP with live video and situational.	Integrated UI enables messaging, playback, and export of relevant footage.
Escalation or Automation	If risk escalates *(e.g. persistent loitering),* automated triggers escalate or dispatch.	Network Rail has immediate visibility and owns the workflow; BTP gains verified intelligence.

To see further integration details see Appendices 3.1.4 and 3.1.5

1 Physical Device layer
2 Network Layer
3 Security Layer
4 Integration layer
5 Software and Analytics Layer
6 Users and Operators

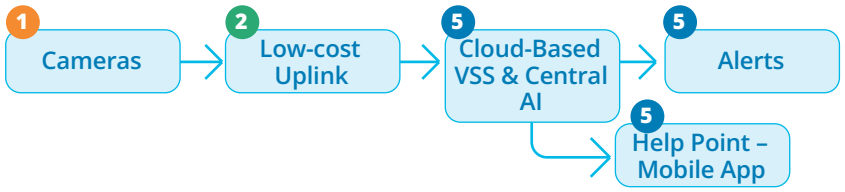
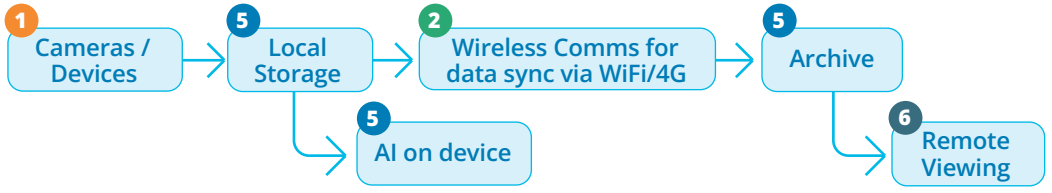
Applying connectivity, cybersecurity, and integration principles ensures that VSS delivers secure, seamless access to footage, whether at high-capacity stations or smaller, remote sites.

	High-capacity stations	Other rail infrastructure (including all other stations)
Data Flow		
Description	The **busiest stations** are characterised by **density of passengers, platforms and cameras, and a complex built environment,** but often with staffed control rooms and on premises NVRs. VSS will have: • Leased Line / SD WAN with 4G/LTE backup. • CCTV infrastructure is supported by Edge Gateways for preprocessing, then local **AI and Cloud-Based VSS systems provide real-time alerting** and analytics. • Data is protected through TLS1.3, AES256 and audit, then mirrored to Cloud-Based VSS for redundancy and central access. • Integrated with control rooms and Cloud-Based SIL platforms, also **providing edge device health monitoring.** Access using Entra ID+MFA, RBAC.	Sites with **lower risk factors** (C-E category stations; 1-4 platforms, simpler layouts, lower footfalls & train density) or **singular risk profiles** (level crossings, bridges): • With FTNx & fibre less likely, cameras **connect via FTTC, WAN or 4G, 5G** centralised Cloud-Based VSS with 4G/5G backup link. • Minimal physical kit to meet DORI guidelines. • **Data is protected with cloud encryption** and local failover. • **Analytics and event/incursion detection is required** and would be undertaken centrally/or on the cloud platform, both visible through RBAC and cloud ACLs. Connect to local PAVA. • Mobile app or help points route alerts to relevant parties and users.
Challenges Met	The technical architecture addresses several challenges at high-capacity stations: • Enables **real-time decision-making** through local alerts. • Using analytics and on-site real-time streaming will help manage a wider range of hazards. • **Reduces dependency** on central systems alone. • Provides network and data resilience through cloud redundancy. • Meets the need for multi-stream recording, real-time alerts, and SIL integration. • Enables staff engagement and **remote BTP access with full audit.** • **BTP and other authorised users** (e.g., Home Office Police or Local Authorities [when jurisdiction neighbours the railway]) **get consistent access.**	The technical architecture **meets and addresses several challenges** at low-capacity stations and across other rail infrastructure: • Limited risk factors mean the cost of large local installations cannot be justified. • For VSS at a site specifically looking for one trigger event, **simple systems with high reliability are provided by this model.** • Requirements for compliance, visibility, & response capabilities are maintained, with special value at locations with more frequent known fatality or trespass hotspots. • Users can have **continuous, remote footage, alert-led live footage or snapshots.** • **BTP and other authorised users** (e.g., Home Office Police or Local Authorities [when jurisdiction neighbours the railway]) **get consistent access.**

2.2.2 VSS STRATEGIC PILLARS

Extending these principles across the wider rail network enables consistent, secure, and seamless VSS access wherever it's needed.

1. Physical Device layer
2. Network Layer
3. Security Layer
4. Integration layer
5. Software and Analytics Layer
6. Users and Operators

	Rail infrastructure sites	Other rail-related VSS
Data Flow		
Description	Similar in execution to cameras within managed infrastructure, but with **additional use cases such as car parks near stations.** This contributes to the future state railway as a backbone to the UK mobility as a service offer: • Minimal physical kit to **meet DORI guidelines.** • Cameras connect via FTTC or 4G, 5G to centralised Cloud-Based VSS or WAN where possible. • Specific event detection such as incursion monitoring or ANPR with **potential for complex situational analysis at edge or on cloud platform.** • Mobile app or help points route alerts to relevant parties.	Numerous locations, on or around the railway, **outside of stations require VSS.** Cameras can be permanent or temporary, train mounted, airborne or body-worn: • Many cameras in this category have occasional power outages, for example forward facing cameras when trains are turned off. **Uninterupted Power Supply** (UPS) should be specified where reasonable to do so. • **Mobile units can record locally and download over 4G/5G** or at fixed site WiFi • Live and recorded feeds fed by 5G into the cloud, mobile app, or local operations centre. • **Edge AI for event or incursion detection** for more complex sites. • Integrated with control rooms for **access by approved stakeholders.**
Challenges Met	The technical architecture **meets, and addresses several challenges** across rail sites: • Simpler installations with lower cost reflect the **lower risk in these sites** to people or the railway. • **Connection to other stakeholders** is possible (e.g., controllers of other transport modes). • Enables **remote diagnostics and low maintenance.**	The technical architecture provides: • Wider visibility across the network to **enable enhanced responses.** • Enables **real-time decision-making** through local alerts to users of Operations Centres. • Provides evidential continuity through cloud redundancy. • System monitoring for power status, sync completion, and error logs. • **BTP and other authorised users get consistent access** without overloading local resources.

3 DEEP DIVE *(Appendix)*

Table of Contents

Strategy Scope

Green / Red line boundaries

This Strategy defines what is **in and out of scope** to drive consistency across the network. It is **intended to be followed by high-priority locations and use cases - particularly those critical to safety, performance, or public confidence.** Whilst non-critical areas, such as certain office environments or lower-priority use cases, are encouraged to follow the standard **where possible.**

Green Line *(In scope)*

Strategy document	Guiding principles for VSS
Timeline	2 Control Periods (CP7 ends in 2029, CP8 ends in 2034)
Locations	High priority locations • Managed Stations / Franchise Stations • Platform ends • Trackside • Safety critical sites (e.g CNI) • Network Operations Centre, The Quadrant, MK Medium/Low priority locations • All other office locations • Depots • Car parks
VSS Types	Station-based CCTV Forward-facing camera & Onboard CCTV Body Worn Video (BWV) Drones Level Crossing CCTV
Use Cases	High-priority use cases • Bridge strike camera • Crime detection/ investigation and counter-terrorism • Crowd management, slips, trips and falls • Gate lines • Staff safety • Vulnerable Presentation & Fatality Management (such as accidental fatalities resulting from trespass or suicides) • Trespass & vandalism
Technology	Medium/Low priority use cases • Asset/track condition or environmental monitoring • Integration with PA/VA Systems • Pedestrian flow monitoring Core capabilities of cameras, i.e. requirements for HD imagery and video Open protocol solutions, enhanced cybersecurity and resilience Cloud-first approach, with flexibility to adopt a hybrid model where appropriate Edge-based technology, remote connectivity and AI Machine/Computer Vision

Red Line *(Out of scope)*

Strategy document	Production of official industry or corporate standards (e.g. NR Level 1 or Level 2) Platform DOO footage Telecoms guidance beyond bandwidth/speed/connectivity options
Procurement	No Preferred supplier list or mandated camera manufacturer
Locations	Private/Heritage Rail or Private Level Crossings

Visual Safety & Security (VSS) is the umbrella term used for camera infrastructure, which includes CCTV and all other visual monitoring systems across the rail network. VSS includes everyday video monitoring such as cameras, screens, networks, security management platforms, body-worn video, mobile (trains/drones) cameras, temporary cameras, and the Cloud-Based VSS. In addition, it includes the supporting capabilities such as analytics, system integration, cloud infrastructure and secure video sharing systems. Together, this ecosystem makes up the VSS systems that are a central part of keeping the railway safe and secure.

APPENDIX

3.1

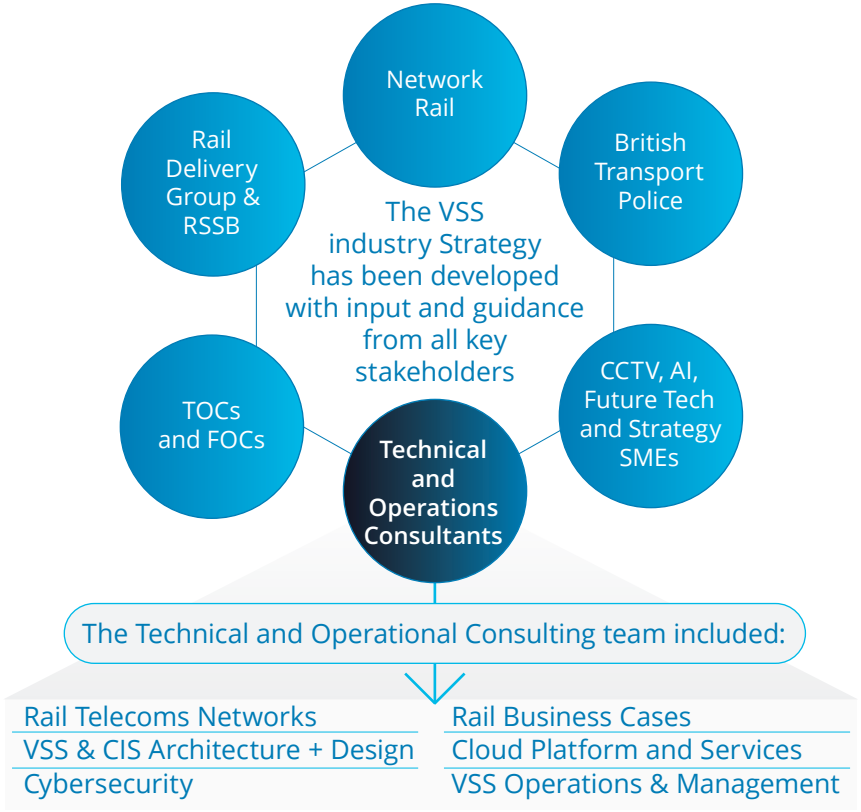
TECHNOLOGY STRATEGY

Introduction: the methods and the purpose of the Technical Strategy

SECTION TAKEAWAYS: The Technical Strategy has been developed from the inputs of all major rail stakeholders.

The Strategy starts with the Industry Vision and the Sponsor's requirements. It breaks these down into the Functional requirements of system users and the Technical requirements of the system itself. This approach ensures that the Strategy will deliver the desired outcomes.

A cross-industry team has delivered the VSS Technical Strategy by connecting the industry vision to a set of common and usable requirements



Vision	The Rail Industry seeks to **enhance the safety, security and performance** of the Railway by integrating the **latest visuals**	**technology,** creating a **unified and connected system for the benefit of people.**
Industry Expectations *(refined through stakeholder engagements)*	The Strategy has been built from the expectations and requirements of the rail industry gathered from **Stakeholder Interviews** (NR, BTP, RDG, RSSB, TOCs, FOCs, etc), **Steering Group Workshops, Document Analysis** and **Literature Reviews** The Strategy incorporated the Rail Delivery Group's	(RDG) Quality, Connectivity, Coverage and Capability framework to yield consistent coverage and interconnectivity. It incorporates connectivity, security and accessibility at its heart with analytics to improve passenger and rail outcomes.
Railway Use Cases + Locations	Users and Sponsors outline their required outcomes: **trespass detection, vulnerable presentation, fatality management, counter-terrorism, crowd management, level crossing clearance, object detection** and **asset management.**	Architectures and information flows were needed for each use case, showing the core principles applied universally and the specific requirements of each outcome.
Functional Requirements	Users' functional requirements were identified during the discovery phase. The included **fewer systems to access, better access to live and recorded data, a smoother experience and stronger cybersecurity protection.** These were used to drive the development of the architecture.	Direct user benefits are outlined in section 6.1. They include improved event awareness through provision of **remote access to live and recorded footage, improved data security through managed and audited access, and superior hazard assessment through real-time visual analytics.**
Technical Requirements	Detailed comprehensively in the technical requirements are **the building blocks for the technical element of the VSS industry Strategy.** Shaped by user needs and functional requirements, these requirements ensure the system is robust, secure and future-ready.	This section shows how the approach to development of the architecture connects technical requirements to the user and the sponsor.

From Vision to Value; VSS Strategy summary shows how the Vision will be delivered by a unified Technical Architecture

Vision

To deliver a safer, more efficient, and future-ready railway system that **strengthens safety and security, enhances performance,** and creates meaningful **benefits for people** through the intelligent use of visual technologies.

	VSS will enhance safety and security	VSS will enhance performance	VSS will benefit people
User Cases	This Strategy exploits VSS to give it a more active role in **enhancing the safety and security** of the railway. VSS Strategy proposes using cameras and analytics to **keep the railway safe from people** by detecting trespass and observing crime hot spots. It will **keep people safe from the railway** by detecting trespass, monitoring incursions, detecting obstacles on tracks, and station hazards. Improving access to video footage will **help First Responders** contain and control incidents to maintain safety.	VSS Strategy recommends analytics and computer vision to **improve situational awareness** and allow a better-informed human response. This will assist the containment and remediation of incidents, while for passengers this means a more **predictable journey time.** **Asset monitoring** for bridges, trackside equipment, and power supplies will reduce operational disruption caused by accidental and malicious interference with the railway.	While rail infrastructure is fixed, people are not. VSS incorporates drones, on-board and forward-facing cameras, as well as fixed cameras. With diverse camera types, VSS Strategy will **support people outcomes** everywhere that people, infrastructure, and trains interact. **Crowd and people analytics** will allow insights for management and the reduction of people-centred risks. VSS will **capture evidence-ready footage** for investigations, insurance, and legal purposes.

Industry Requirements and Benefits

VSS must build on the rail's current VSS estate to become a **unified and connected system** with a common **design specification.** The system must also **comply with relevant standards.**

The benefits will be a **safer railway** and an **enhanced passenger experience.** There will be reduced impact from the unplanned events that cause operational disruption.

Users of this Strategy

GBR / TOCs: To support the industry's pivot to more passenger-centric rail service.

British Transport Police: Beneficiaries of improved connectivity and access to VSS footage

Asset Owners: To replace and upgrade VSS infrastructure in respective regions.

NR DDaT or TOC Equivalent: To identify user requirements for data management and cloud storage.

NR Technical Authority or TOC Equivalent: To establish architectural principles for new sites and relevant inputs for new standards or training.

VSS Functional Requirements must be delivered in a usable, resilient, and available system to support system adoption

The Functional Requirements in the previous slide are underpinned by these fundamental design considerations. These are embedded in the system architectures.

ACCESS MANAGEMENT

The proposed technical architecture is designed to **deliver the best balance between access and compliance.** Remote access to live and recorded feeds will **support situational awareness and decision making,** but must be controlled according to role, person, and organisational permissions. Ethical and legal considerations will always apply.

RESILIENCE

Operational resilience is a **cornerstone of the technical architecture.** Reliability, Availability and Maintainability are delivered through redundancy of essential systems, providing **resilience to shocks,** whether environmental, human, technical or force majeure.

AVAILABILITY

The architectural choices and solutions ensure high system availability to **improve the reliability of the VSS systems.** Management systems with ITIL for service management, along with sub-systems featuring diagnostic health reporting, are specified.

MAINTAINABILITY

To reduce any downtime, **ownership of maintenance responsibility is required.** While we envisage maintainability to be shared across the industry, there are key organisational roles to be played by Network Rail.
At the operational level, **a complete asset register is required** to clarify maintenance responsibilities.

DELIVERY

Delivery of the functional requirements is dependent on an **integration layer (SIL – Security Integration Layer) between edge assets and users.** Maintenance systems that register assets and measure their health will **support the delivery of Asset Management targets.**

Users' requirements for VSS are broken down into Functional Requirements that should be used to define future VSS systems

Any system, regardless of its potential, will only be widely adopted and maintained if it meets user requirements.

These Functional Requirements must be used to specify future VSS systems to ensure strategic compliance.

I need video images that are clear and usable

Must provide an intuitive and accessible user interface and experience across devices.

Images and events **must** be visually distinguishable under variable lighting, weather, and environmental conditions (e.g. rain) to support situational awareness and enable timely decisions.

Should comply with the Detection, Observation, Recognition, and Identification (DORI) framework.

I need timely access to footage

Real-time and recorded footage **must** be available to authorised users with minimal delay, regardless of location.

Must support role-based prioritisation of footage (e.g. BTP access to critical footage during incidents).

Must detect and report events and hazards instantly.

Could allow for access to footage in the event of degraded working conditions.

I need systems to be compatible

Must be compatible with other 'protection' systems, such as perimeter measurement systems, obstacle detection and passenger-facing systems such as PAVA.

Should support commonly used video standards (e.g., MP4, H.265) and integrate with evidence management tools, archival platforms, and analytical software without requiring conversion.

I need VSS systems to be built on existing technology

Must interface with existing 'control' systems (e.g., command and control tools, legacy cameras, third-party analytics) with minimal retraining or business disruption.

Must enable integration with third-party systems and future technologies, for example, by using open APIs and ONVIF compliance.

Should enable a repeatable 'GBR-ready' architecture, able to grow and adapt to future needs without vendor lock-in.

I need the VSS System to be resilient

The system **must** be resilient, including back-up for critical functions and alerts provided in the event of system failure.

Should continuously monitor system performance, provide remote self-diagnostics and raise alerts to reduce operational costs and carbon footprint.

I want to lower the environmental impact

Should be designed to minimise energy use and asset base without compromising performance.

Could provide for power-aware operation, intelligent device scheduling to reduce power consumption.

My VSS system must be secure

Must implement strong security measures such as encryption, firewalls, and regular updates.

Must ensure compliance with data protection standards.

Must ensure only authorised users can access the system.

The Technical Requirements will deliver the unified, scalable and resilient industry-wide VSS capability required by the Strategy

These Technical Requirements must be used to specify future VSS systems to ensure strategic compliance.
They have been agreed upon by all stakeholders and combined with the Functional Requirements to deliver the Industry Vision.

1/2

Detect Hazards, Incursions and Anomalies

Where the use case requires, the system **must** provide analytics for real-time detection of hazards, providing alerts for human response or through connection to other systems, e.g. Voice Alarm.

Provide Secure Access

For observation of real time and recorded footage, including for evidential purposes, the system **must** use encrypted streams (e.g. VPN/AES-256) with secured access, such as multi-factor authentication (MFA), single sign-on (SSO), role-based access control, session timeout, and audit logs.

Resilient Connectivity

The network Connectivity solution **must** provide high levels of reliability, availability and maintainability. For example, through effective redundancy, SD-WAN integration, MPLS-ready design, FTNx support for high bandwidth areas, and wireless fallback where wired connectivity is unavailable.

Facilitate Future Scalability

The system **must** be vendor-agnostic and cloud-ready, with support for local storage, new analytics tools, and AI services.

Monitor Video Safety System Health

Should provide monitoring tools with automated fault detection, remote diagnostics, and reporting - including predictive analytics for system health.

Integrated Systems and User Experience

Must integrate cameras, storage and user interfaces to deliver the functional requirements. Open APIs, ONVIF compliance, support for common data models (JSON, XML), and vendor-agnostic data exchange are expected.

Should provide remote control of fixed (i.e. PTZ) or aerial cameras (i.e. drones) where the use case requires.

The Technical Requirements will deliver the unified, scalable and resilient industry-wide VSS capability required by the Strategy

These Technical Requirements must be used to specify future VSS systems to ensure strategic compliance.
They have been agreed by all stakeholders and combine with the Functional Requirements to deliver the Industry Vision.

2/2

Zero Trust and Cybersecurity Built In

Zero-Trust architecture principles **must** be embodied in the design - for example, network segmentation, access control, encrypted data at rest and in transit, endpoint protection, regular patching, vulnerability scanning, and security audits.

User-Friendly Experience

User experience **should** be intuitive, avoiding disruptions to access and inconsistency across systems.

Must include a web-based interface and mobile access that provides clear and actionable alerts, along with simplified workflows for users.

Connected System

VSS **must** be remotely viewable in chosen locations, which may include NOC, ROCs, TOC Control Centres, and in specified sites for vital industry stakeholders, including BTP.

Must provide authorised users with access to real-time and recorded footage for observation and control.

Resilient System

System **must** meet RAM targets, which could be delivered through provision for an uninterruptible power supply, remote monitoring duplication, hardware architecture, automatic failover mechanisms, disaster recovery processes, and continuous uptime monitoring.

Usable and Protected Image Data

Image quality **must** be considered in design by applying DORI Guidance.

Data **must** be protected by technical solutions (e.g., AES-256 encryption, secured hardware, access controls) and by processes (e.g., data retention, GDPR compliance, data privacy standards).

Compliant System Design

System **must** be compliant with applicable stakeholder standards, national legislation, and relevant national standards for the management, operation, and monitoring of CCTV in public places.

APPENDIX **3.1.2**

CONNECTIVITY APPENDIX

SECTION TAKEAWAYS:

Network connectivity selection will be influenced by location and bandwidth requirements.

FTNx has ample capacity, but its expense and availability mean that the corporate network may be preferred in stations, while 5G networks may be preferred in remote locations.

Connectivity options have been identified to support the specification of future installations

Each deployment will have different connectivity restrictions and requirements, connectivity options are provided across the **'network layer'.**

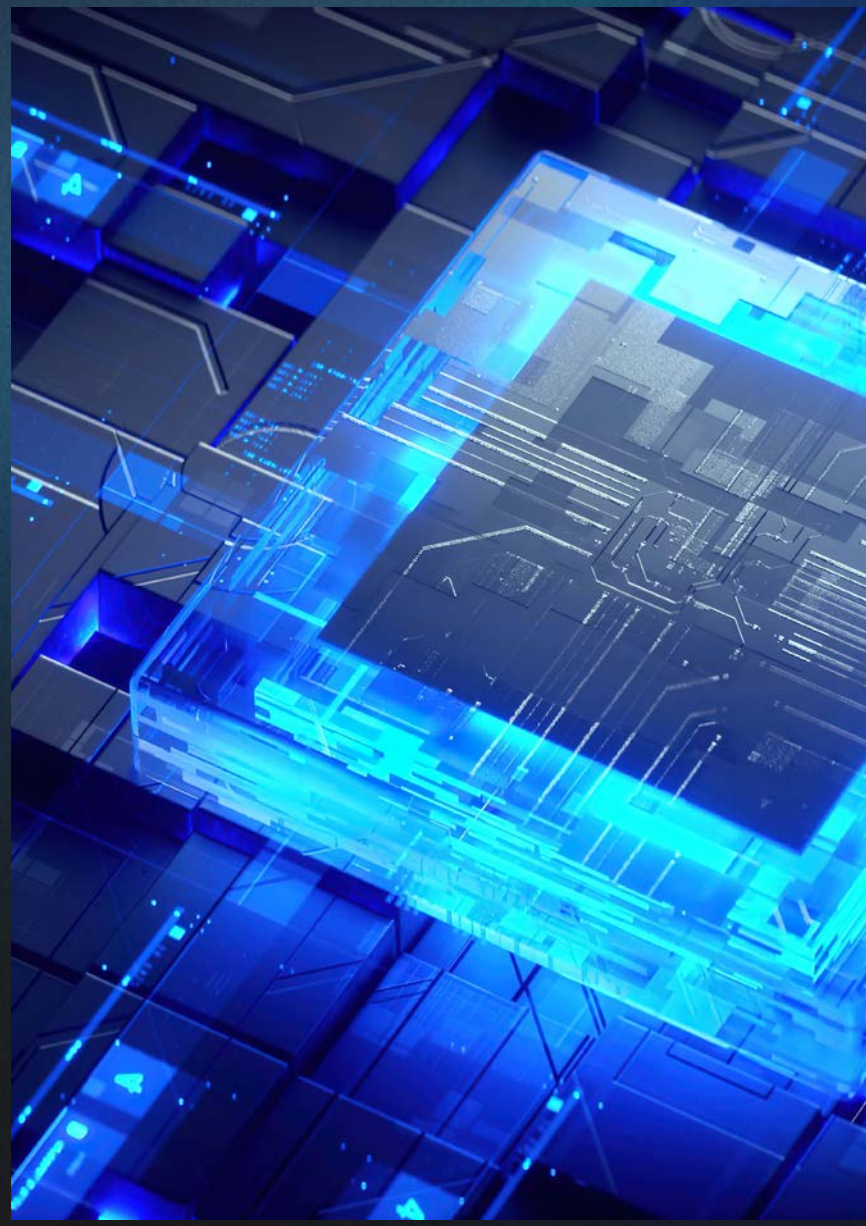
	Bandwidth	Deployment Complexity	Security	Reliability	Cost	Sustainability	Scalability	Spares Availability	Potential Use Cases
Wireline (fixed line) Product from Service Provider	100 Mbps	Medium	High	High	Low	High	Medium	N/A	Remote locations*
On Net (FTNx) where available	Upto 1Gbps	Low	High	High	High	High	High	High	Stations
Fibre to On Net where FTNx is not available	Upto 1Gbps	High	High	High	High	High	High	High	Remote locations* (nearby FTNx)
Project Reach Fibre connectivity	Upto 1Gbps	High *(development currently underway)*	High	High	High	High	High	High	Portfolio to be developed (incl. sites without FTNx)
Wireless MNO	15 Mbps (UL)	Low	Medium	Medium	Low	Medium	Low	N/A	Drones, Forward facing CCTVs
CUE (Corporate Network) or SD-WAN for Stations	2 Mbps to 1 Gpbs	Medium	High	High	Medium	High	Medium	High	Stations
High Bandwidth Station WiFi**	Upto 1Gbps	Low	High	High	Low	High	High	High	Onboard CCTV to download at station

** Remote location could include any lineside site of interest, for example, plain line vulnerable to cable theft, REB, signal box, bridge, level crossing*

*** Using station wifi to transmit images of passengers from on-board systems to a central Cloud-Based VSS will only be possible if the network has the policies and protections required to fulfil the commitments of GDPR.*

APPENDIX **3.1.3**

CYBERSECURITY APPENDIX



SECTION TAKEAWAYS: The connection of visual data to users requires that the technical architecture is aligned to Zero Trust principles, and cybersecurity controls are built in.

Cybersecurity for a national VSS network: industry-level risks and mitigations

Two key risks are most relevant to the cybersecurity of the VSS system.

The UK Rail cybersecurity estate is characterised by significant capability and protection, often delivered by autonomous and devolved procurement. Solutions can be implemented faster, but **the trade-off is a loss of architectural commonality and management rationale.** For example, Transport Layer Security (TLS) protocol version 1.2+ or higher ('1.2+') is enforced as a security policy to ensure secure data transmission between cameras, NVRs, servers, etc., in the current and future state architecture across the rail industry. Often, security solutions are procured, but **their functionality is not exploited,** which may open gaps in the continuous coverage of installed solutions.

Connecting the estate increases the 'attack surface' and poses a greater threat to both the system's functionality and recorded images.

The technical Strategy's solution to these risks is to **ensure that cyber risk is managed to As Low and Reasonably Practicable ('ALARP'), within a Zero Trust Framework.** To achieve this, **a unified set of functional requirements** has been taken and translated into the controls needed and their associated Zero Trust Principles. This approach will support the specification of all new VSS procurement and deployment.

APPENDIX **3.1.4**

INTEGRATION APPENDIX

SECTION TAKEAWAYS:

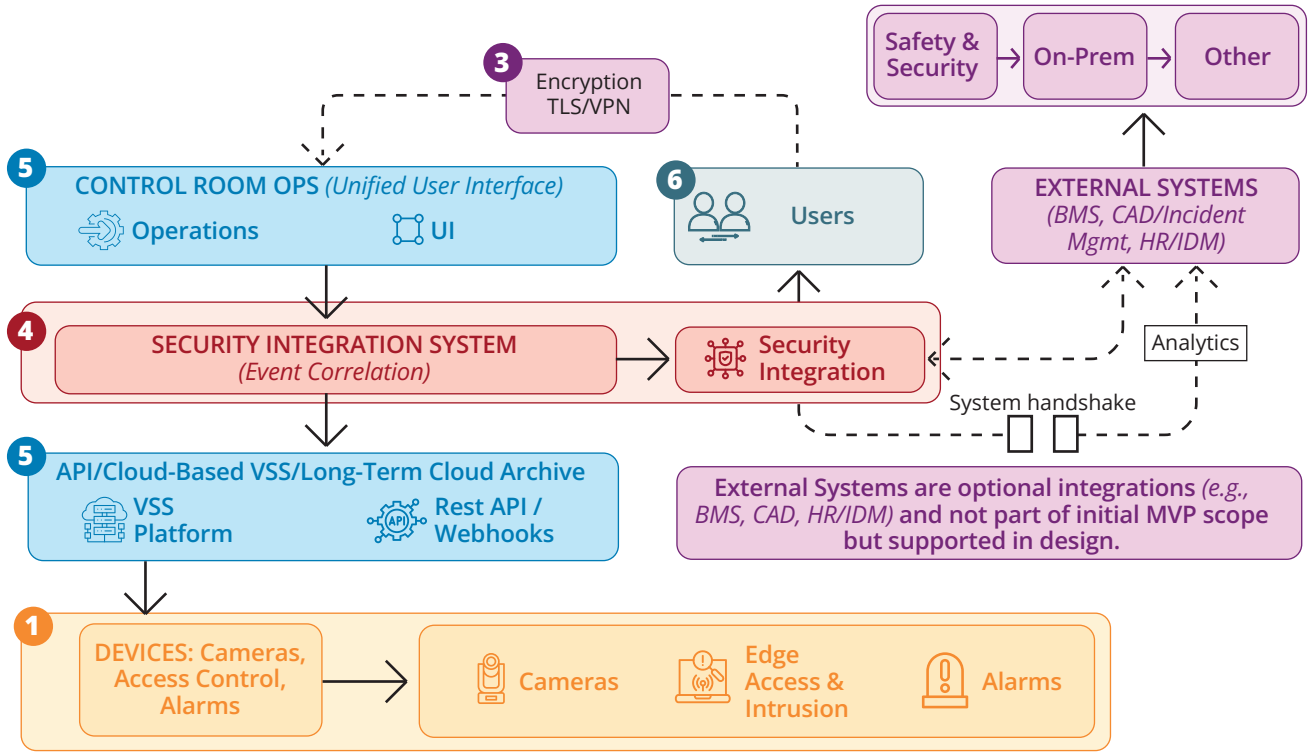
Integration of edge devices to users should be delivered by a Cloud-Based Security Integration Layer (SIL). This allows a clean flow of alerts and visual information to improve situational awareness and reduce risk.

Analytics on edge or Cloud can provide superior hazard management.

Data can be stored with backup in the Cloud.

The integration of edge devices is central to the VSS industry Strategy

This diagram explains how the industry can connect information from different VSS systems using a **Security Integration Layer** to provide a single view that operators can use in a control room, or remotely through a secure user interface:



1 Physical Device layer
2 Network Layer
3 Security Layer
4 Integration layer
5 Software and Analytics Layer
6 Users and Operators

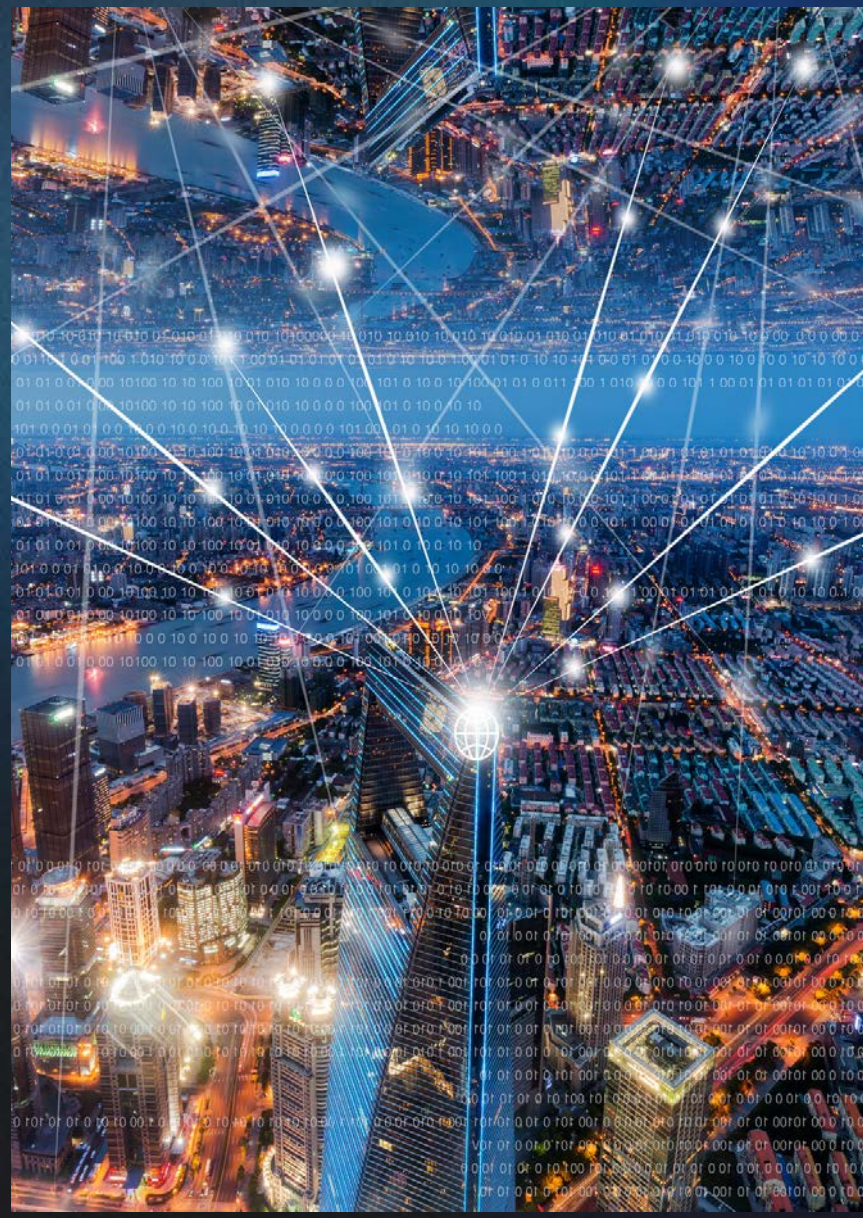
The Integration Layer between edge devices and users should be specified. A Cloud-Based Security Integration Layer, is recommended.

The table below provides a high-level comparison between using a full Cloud-Based Security Integration Layer solution, an intelligent Cloud-Based VSS, or having no central platform.

Options	Pros	Cons
Cloud-Based Security Integration Layer *(SIL)*	Centralised control and coordination Integrates CCTV, alarms, access & analytics Policy-based workflow management Proven in multi-stakeholder rail environments Scalable and vendor-neutral	Additional licensing and integration costs Potential overlap with existing systems Requires clear configuration to avoid complexity
Alternative Management Layer *(intelligent Cloud-Based VSS or custom orchestration)*	Lower cost than full Cloud-Based SIL Retains automation and basic workflow logic Can build on existing infrastructure Flexible and scalable with fewer vendor constraints	May lack full situational awareness capability Design effort needed to match SIL functions Integration & audit features can vary
No Central Platform *(manual or localised)*	No added licensing or platform complexity Simple to operate in small or isolated environments	No coordinated workflow or escalation Weak auditability and handover Limited support for national-scale coordination Higher risk of data inconsistency or loss

APPENDIX **3.1.5**

CONTROL ROOM APPENDIX



SECTION TAKEAWAYS: VSS should be delivered to the distributed network of existing Control Rooms and remotely to approved users since costs and resilience are improved over routeing to a specific new build Control Room.

VSS Strategy recommends distributed Control Room functionality to achieve lower cost and greater resilience

The Strategy recommends feeding VSS images to existing Operations Centres and to remote users, rather than to Operations Centres alone. The Appendix provides examples of a similar 'distributed model' deployed in other Infrastructure-heavy industries.

Distributed Control Room functionality delivers these Functional Requirements:

- Image Usability
- Timely Accessibility
- Format Compatibility
- System Adaptability

...and these Technical Requirements:

- Future Scalability
- Monitoring System Health
- Integrated Systems & User Experience
- User Friendly Experience
- Connected System
- Resilient System

		Centralised Control Rooms; feeding VSS insight to purpose-built rooms with secure access	Distributed Control functionality; feeding VSS insight to purpose-built rooms with secure access
Cost	By leveraging existing cloud infrastructure and Network Rail's Cloud-Based SIL/VSS platform, a distributed model has a lower whole life cost and reduces CapEx. It allows flexible, scalable operational expansion.	High upfront CapEx; costly to scale and often high vendor lock in.	Lower Capital and initial costs; pay-as-you-grow.
Complexity	Integrating various systems (e.g. CCTV, alarms, lifts, SCADA, access control) within a unified interface introduces inherent complexity. The distributed model partly mitigates this by standardising secure API-based access, centralised orchestration, and reducing dependency on point-to-point integrations. RBAC, SSO and MFA further simplify and secure the operational environment.	Low at outset; increases with scale.	Moderate to high integration effort which better matches modular, cloud-based architectures.
Scalability	The rail industry's national footprint requires an approach that supports regional autonomy while maintaining overarching strategic control. The distributed control capability enables local teams to act quickly and decisively, while aligning with central policies.	Difficult; site expansion is physical.	Easier; scale by user and access point. Enables rapid regional or national coverage.
Resilience	Traditional control rooms may be vulnerable to physical disruption or local outages. In contrast, the distributed control capability is designed to remove single points of failure with failover protocols and automated switchovers to duplicate systems, geo-redundant cloud hosting, Disaster Recovery environments.	Vulnerable to single site outage.	Geo-redundant access, multi-node fallback. Stronger continuity in adverse events.

Developing the 'Control Room function' creates an operational advantage for rail stakeholders and improves service for customers

The Railway's Strategy sets out the technology and capability that enables control by routing the real-time and recorded images to any location to improve situational awareness & provide the insights required for operational control. Adding the 'control room function' for VSS system users has a host of defensible advantages, including operational resilience, cost avoidance, reputation enhancement and control of the system itself.

BENEFITS

Benefits to the sector	Benefits to Network Rail and other undertakings	Benefits to the passenger
Enhances resilience by democratising VSS streams and applying a coherent cybersecurity approach.	Combines CCTV, sensors, alerts, and event logs into a single interface to support shared situational awareness.	Better utilisation of the existing VSS estate will enhance passenger safety without creating a sense of increased surveillance.
Improved visibility of the asset base enables better insight and control.	Directly supports use cases such as live streaming, incident logging, response coordination, audit, search, and supports proactive, prevention activity.	A step change in hazard identification and analysis will help eliminate some situations. Enhanced provision of incident insight will accelerate reversion to normal.
VSS is GBR-ready, bringing the entire system and the data it processes under unified, coherent governance, through aligned policies, standards, and management.	Integration enables remote co-ordination with other systems, including Building Management, SCADA, and PAVA.	Greater confidence in rail service stemming from enhanced staff training, support and role clarity ensuring new systems are adopted without impacting day-to-day operations.

CONSIDERATIONS

Expected costs and effort
Initial investment in systems, maintenance and support.
Governance frameworks, e.g., station environments such as Stratford Station, where multiple undertakings operate within the same space.
Integration costs to link legacy and third-party CCTV to Cloud-Based SIL and VSS platforms.
Costs to support user adoption, expectation setting and time for training.

While BTP has among the best current rail control room functionality, this proposal will enhance even their capability in the following ways:

Aspect	Current British Transport Police Functionality	Proposed Control Room Functionality
Primary Purpose	Evidence gathering, and post-incident response	Operational resilience, infrastructure safety, incident management
Access Level	User-level access; read/view permissions vary by stakeholder agreements	Full administrative ownership with multi-agency user privileges
Systems Coverage	Predominantly CCTV access; limited integration with other systems	CCTV, alarms, lifts, PA, SCADA, analytics, incident tools *(Security Integration Layer)*
Data Retention & Policy	Governed by BTP's internal evidence protocols & criminal investigation procedures	Governed to railway standards & GDPR obligations
Live Feed Access	Aspires to estate-wide access; currently limited by third-party restrictions	Comprehensive access, subject to permissions
Recorded Footage Access	Often delayed; requires footage request or indirect access via Network Rail or TOCs	Near-immediate access across cloud, edge, or local retention systems
Incident Escalation Flow	Triggered by external notification or request no direct automation capability	Triggered by Network Rail operators or automation
Automation Potential	Limited; analytics not integrated directly with operational workflows	Full integration of AI analytics for detection, triage & escalation
Strategic Alignment	Supports investigation but lacks the scale or integration for broader rail Strategy	Enables delivery of cross-agency requirements
Security & Governance	Security depends on remote interface & manual logging	Central role-based control

APPENDIX **3.1.6**

VSS ARCHITECTURE FLOW DIAGRAMS APPENDIX

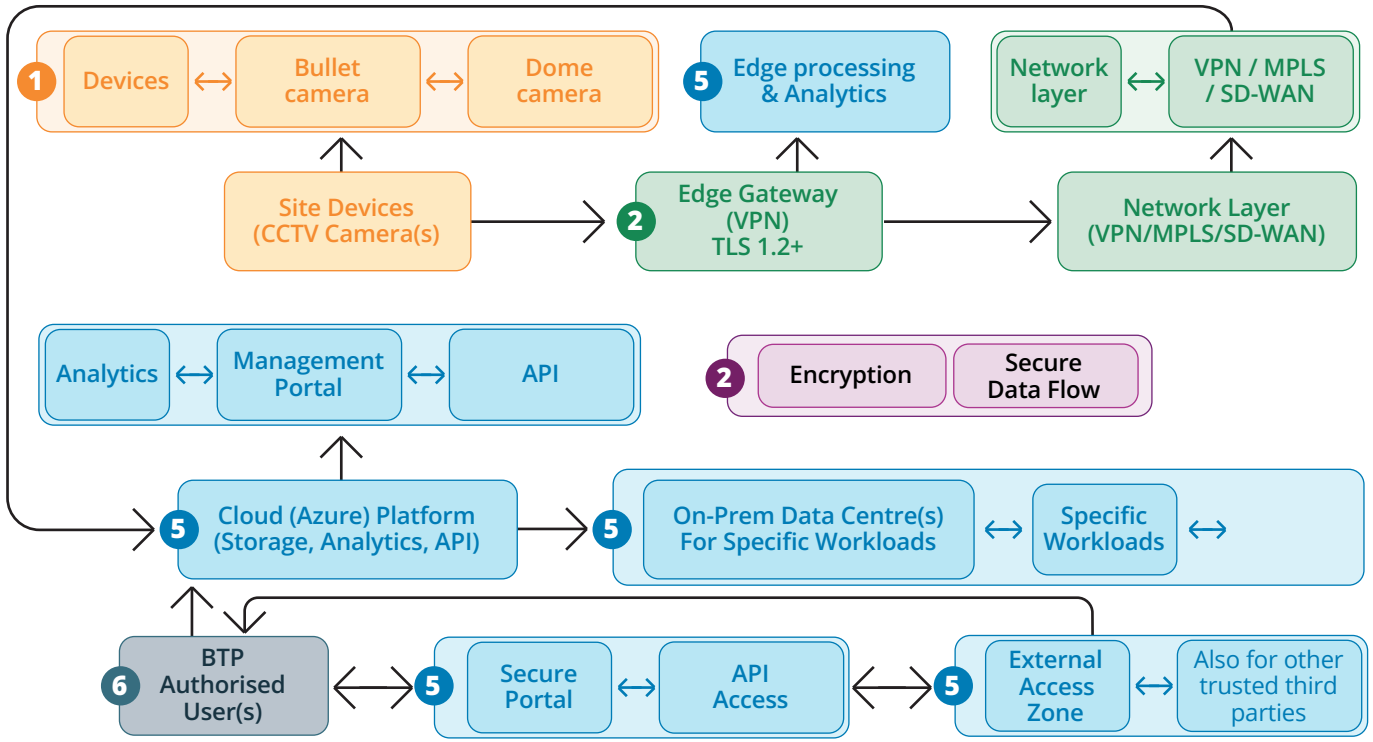
SECTION TAKEAWAYS:

On premise and Cloud platforms can provide an optimum mix of availability – through secure remote authentication of all users – and resilience – through redundancy.

Deploying edge and Cloud analytics capabilities provides immediate hazard assessment.

VSS architecture promotes the flow of information from edge devices to users.

The VSS architecture creates new communication channels from the camera to the users



1 Physical Device layer
2 Network Layer
3 Security Layer
4 Integration layer
5 Software and Analytics Layer
6 Users and Operators

The connections between key sub-systems are required to ensure strategic compliance. This VSS architecture diagram shows how cameras, cloud and on-prem platforms, and authorised users, including BTP, are connected, and **where information flow dominates.** This view can be used as a basis to define the information flow for any use case.

CCTV Cameras at Sites: Bullet, dome and PTZ cameras transmit footage using TLS encryption.

Edge Gateway & Processing: Local Edge Gateway processes, compresses and encrypts – with potential for analysis – for secure forwarding to the Network.

Network Layer: Transports encrypted streams; supports VPN, MPLS, SD-WAN according to local preference with TLS 1.2+ for end-to-end protection.

Cloud Platform: Storage, analytics, and system APIs can be delivered with high availability, scalability, and ease of integration.

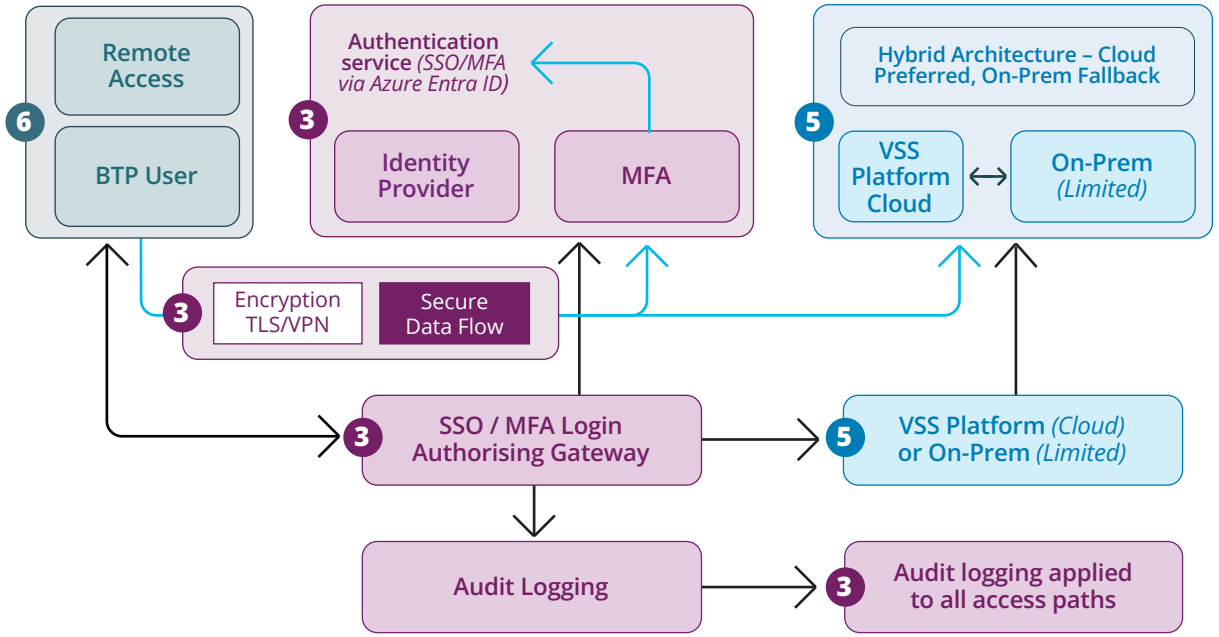
On-Prem Data Centres: With significant legacy storage, the platform will connect to local VSS for local storage and processing.

Authorised User Access: External organisations like BTP can be authenticated by SSO and MFA to access the API.

Data Commands: Enables control commands from authorised users back to devices (PTZ, presets, start/stop, DO triggers).

The VSS Architecture allows for railway organisations and railway partners to access footage remotely

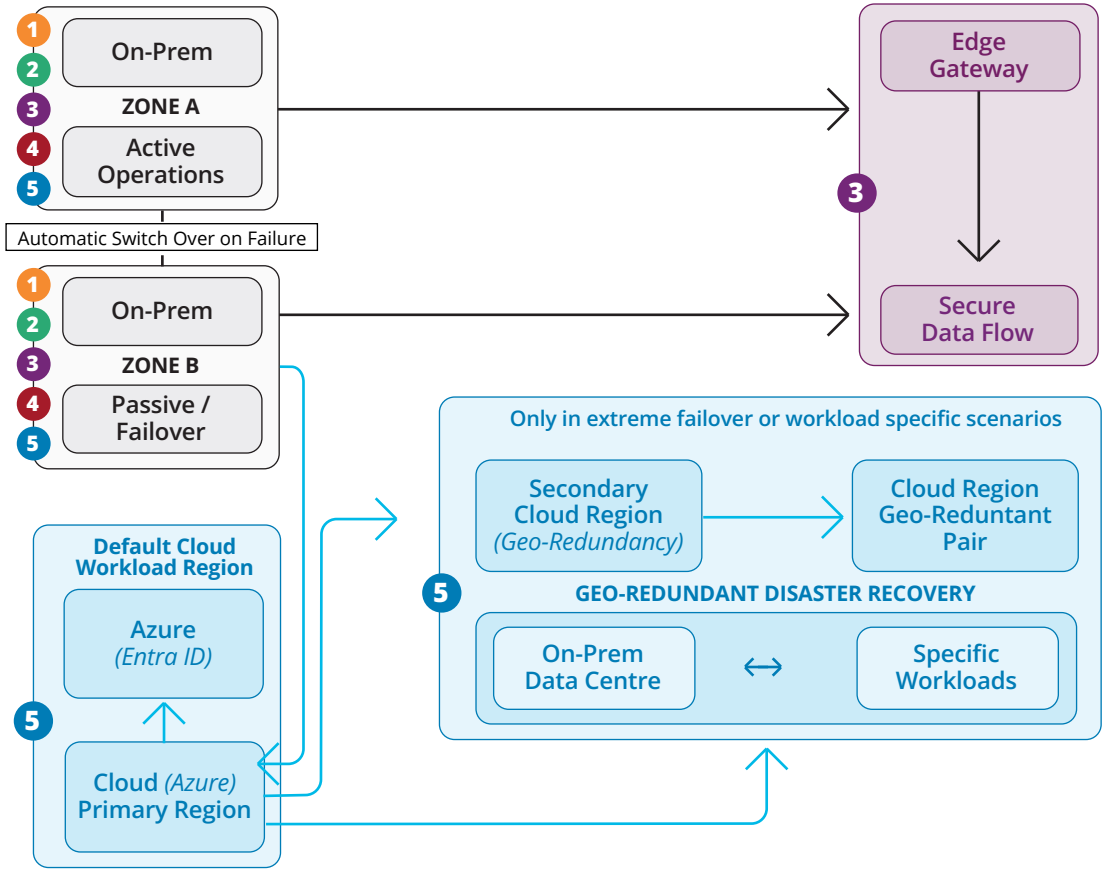
The data flow diagram below outlines how BTP or other permitted agencies can securely access the VSS Systems using a controlled pathway, showing how both railway organisations and railway partners interacts with CCTV footage.



User	Primary Interest	Access Model	Information Sharing	Changes Made
Rail providers	Ongoing infrastructure monitoring, safety, remote analytics, and real-time operations.	Persistent and full access.	Proven comms protocols embedded in Cloud-Based VSS /Cloud-Based SIL & RBAC define access levels. Options for info exchange are federated access via Cloud-Based SIL/VSS, secure shared portals or direct VoIP/ secure landline bridging.	Common standards & architecture means repeatable roll-out & easier integration into central VSS.
BTP and other rail partners	Incident-based response, law enforcement, evidence retrieval.	Situational. Authentication to shared integrated VSS by Azure Entra ID (SSO + MFA) using BTP email.		Rail partners authenticate with their own identities into central VSS, then have access to footage without travel to site.

1 Physical Device layer
2 Network Layer
3 Security Layer
4 Integration layer
5 Software and Analytics Layer
6 Users and Operators

The VSS data flow and storage are resilient by design



1 Physical Device layer
2 Network Layer
3 Security Layer
4 Integration layer
5 Software and Analytics Layer
6 Users and Operators

This diagram addresses VSS data resilience through a combination of on premises and cloud-based systems for disaster recovery. The resilience of edge devices will be separately enhanced through self diagnosis and reporting enabled through the connected network.

Through a system availability lens, the VSS architecture has:

Two physical data centres: used with automatic switch-over, Site A (Active) runs the live service while Site B (Passive) is on standby as a fail-safe.

Edge gateway connectivity: Each site can route data between devices and platforms.

Secondary cloud region for redundancy: Critical data is also replicated to a secondary (geo-redundant) cloud region, protecting the system in case of a failure in the primary cloud.

Optional On-Prem disaster recovery site: For sensitive workloads that require on-site control, a dedicated on-premises disaster recovery setup is included.

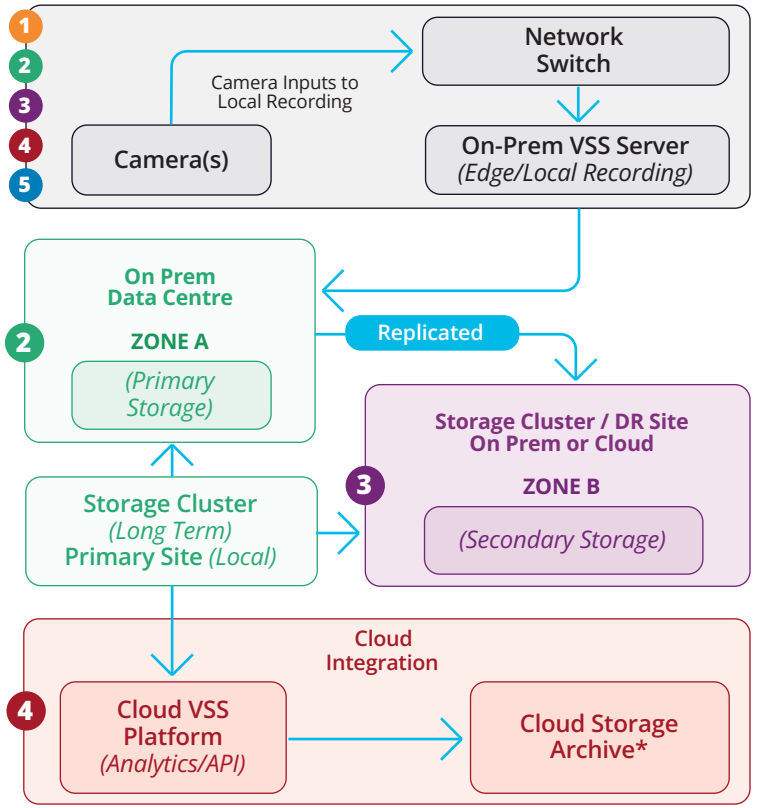
Secure, bi-directional data flow: All communication across systems is secured.

Primary cloud region: The platform is connected to a secure Azure cloud region.

While implementing redundancy incurs additional costs that may not be justified for all use cases, it is essential for systems impacting operational railway functions. Leveraging a Cloud connection as a redundant layer alongside on-premises storage helps reduce availability risks to ALARP (As Low As Reasonably Practicable).

The VSS architecture can create a resilient data environment using local and cloud capabilities

The VSS platform diagram highlights how a **hybrid model combining 'on-prem' infrastructure with cloud-based services** ensures high availability and security.



**It will be the decision of individual organisations on what data they wish to store*

The VSS architecture delivers data resilience by:

Edge Recording & Local Access: Cameras transmit to local VSS servers immediately.

Primary Storage (Zone A): Footage is automatically pushed to on-prem storage clusters for short-to-medium term retention.

Secondary Storage (Zone B): Data is replicated on-prem or at cloud-based disaster recovery sites.

Cloud VSS Platform: Data is streamed or batch loaded to Cloud VSS, providing data resilience but also more opportunities to analyse images.

Cloud Storage Archive: For low-cost retention, footage is archived on 'Blob' storage.

There are clear operational advantages to this approach:

Modular Expansion: Add storage, compute or bandwidth without disruption.

Cloud-Read: Cloud services are already integrated and policy-driven.

Vendor-Agnostic Design: Based on open standards, supporting procurement freedom.

This approach balances the prevalence of local infrastructure with the scalability of cloud services:

Hybrid by Design: Choose what to store locally, replicate offsite, or push to cloud, offering control over costs, bandwidth, and policies.

Full Cluster Compatibility: Supports active-active clusters or active-passive replication to suit different resilience needs.

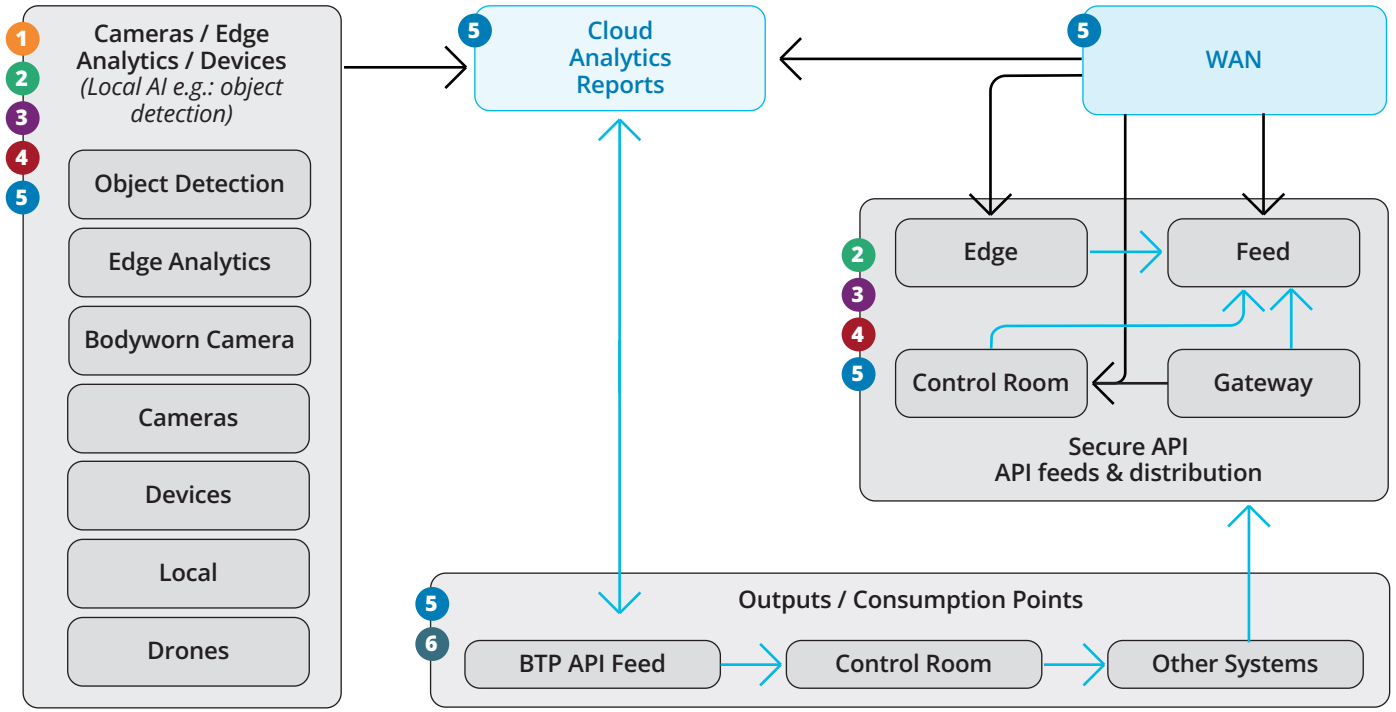
Workload Segregation: Local clusters manage immediate footage; cloud services support analysis, export, and investigation workflows.

The **benefits** this architecture has for **railway organisations** include **consistent availability** of footage across sites, **centralised access** via the Security Integration Layer, multi-operator **retention & control with audit logs,** and disaster resilience to protect operational resilience. For BTP, **benefits** include eliminating the delay from manual exports or retrievals and **searchable footage** with tags & alerts.

1 Physical Device layer
2 Network Layer
3 Security Layer
4 Integration layer
5 Software and Analytics Layer
6 Users and Operators

Using a cloud-based VSS architecture will allow analytics to be performed network-wide in a secure environment

This VSS platform diagram highlights how the architecture **integrates edge-based video capture and analytics** with centralised cloud processing to deliver actionable insights across the network. Analytics plays a pivotal role in the delivery of the Strategy's Functional Requirements – in particular, real-time insight and faster remediation of incidents.



Pilot studies in London Bridge have provided valuable insight.

Data is processed at the location of greatest convenience:

Edge Inputs & Local AI: Cameras may operate with embedded fixed analytics (e.g. object detection, activity monitoring). This reduces the volume of video transmitted to central systems.

Edge to Cloud Analytics Pipeline: Edge data flows securely into the Cloud Analytics Report platform via encrypted WAN links, where AI/ML insights can be generated with low latency. The costs associated with high bandwidth transmission can be mitigated by deploying edge analytics as far as possible.

Secure API Feeds for Consumption: Dedicated BTP API feed allows authorised, auditable access to filtered analytics for policing and incident support. APIs also serve control room users and other systems such as the Security Integration Layer, operational dashboards and external intelligence tools.

1 Physical Device layer
2 Network Layer
3 Security Layer
4 Integration layer
5 Software and Analytics Layer
6 Users and Operators

APPENDIX **3.1.7**

DEPLOYMENT AND CAPABILITY ROADMAP APPENDIX

SECTION TAKEAWAYS:

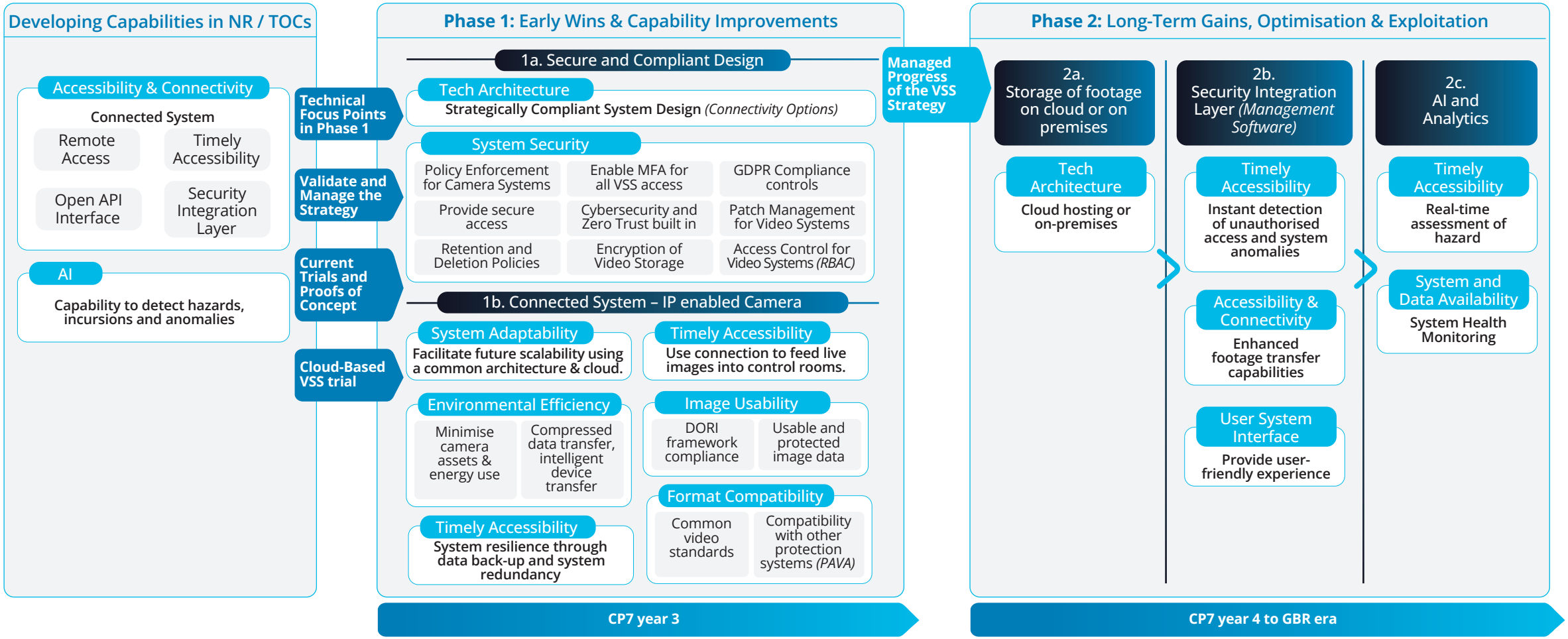
Securely networking cameras and using cloud or Data Centres to provide video management, analytics, and storage will enable delivery of compliant VSS.

Adding integration through a Cloud-Based SIL from end devices to users – working in distributed Control Rooms or on individual devices – will deliver the benefits of VSS.

Below is a possible technology capability roadmap, starting with early wins, capability improvements, and then gradually shifting focus towards long term gains, which supports the transition to a more interconnected railway era.

Adoption of the Strategy by Asset Owners for the local sites to re-equip existing life-expired assets.

Strategy adopted by the industry in preparation for GBR for the benefit of passengers and UK rail.



The Technical Capability Roadmap shows a phased approach to improved VSS capability

By separating the road map into capabilities, the strategy can be more easily adopted and delivered, since each capability is owned by a discrete part of the industry.

Big Themes	**Phase 1** 'Quick Wins' (validated architecture, connectivity, resilience, stakeholder confidence)	**Phase 2** 'Integration and Optimisation' (integration between users & assets, improved situational awareness, data & connectivity back-ups, analytics, enhanced hazard reduction)		Ongoing
Connectivity (WAN, FTNx, SD-WAN, 4G)	Validation of primary and fallback models	Standardisation across VSS estate	Performance tuning & expansion	Network refresh and upgrades
BTP Access (API/Feeds)	PoC with selected sites and officers	Scaling to national and remote access	Interlinking with command systems	Continuous audit and role review
Edge Analytics	Deploy with body-worn video or drones at pilot sites	Included in rural and high-capacity kits	Refinement and use case expansion	AI model updates and alerts calibration
Cloud Integration (Cloud-Based VSS/ Storage)	Hybrid Cloud-Based VSS and retention tests	Rollout of cloud-first or 'cloud as back-up'	Cross-platform analytics and dashboard	Retention reviews, cost tuning and costs benefits of data centre vs cloud
Cloud-Based SIL and Dashboard Integration	PoC-level API triggers and alarms	Wider API feed and operational alerts	Multi-source insight and escalation	New sites added, new capabilities (PAVA integration) and system diagnostics
Security Controls	RBAC, TLS, MFA tested in pilot. TLS 1.3, AES 256 encryption for all transport-layer communications	Enforced as standard via Entra ID	Audit, zoning and privilege policies	Cyber reviews, red teaming, aligning with NSCC cyber assessment framework – reference NIST800-53
Partner Access (TOCs, Third Parties)	Scoped trials for different user groups via federated login	Controlled rollout with retention limits	Shared insight via secure APIs	Usage audits and scope expansion

APPENDIX

3.2 FUTURE TECHNOLOGY TRENDS

SECTION TAKEAWAYS: This section outlines the strategic technology domains and innovation trajectories that will shape the evolution of VSS Systems across the rail industry. Leaders and Asset Owners should use this model to explore emerging capabilities, anticipate implementation challenges, and foster collaborative planning across stakeholder groups. Structured around a horizons-based framework and supported by capsules of insight, the model enables organisations to align on plausible futures, trial new solutions, and operationalise technologies up to the next 15 years.

Key trends in the future of VSS

Proactively addressing identified risks and operational constraints is essential to unlocking the potential of emerging technologies.

By anticipating and managing implementation challenges, the industry can create the conditions necessary for successful future technological adoption.

Understanding the future technology landscape will allow the Rail industry to plan its path towards it.

As part of the Visual Safety & Security (VSS) Strategy development, a horizon scan was conducted to identify emerging technologies with strategic relevance to the Rail Industry.

The accompanying projections highlight transformative changes anticipated to be unlocked within the lifespan of the Strategy.

These projections are plausible, rooted in existing technological capabilities and follow realistic evolutionary trajectories over the coming years.

Throughout the scan, convergence is a key and defining characteristic which will influence many, if not all, future VSS solutions. Each solution area suggested blends advancing technologies (almost always including a form of AI) to create an enhanced, superior solution.

Smart Spaces and Capabilities

Democratised AI, growth of digital twins, exploitation of new data sources such as satellite and fusing of insight from IoT devices and other sources will combine to deliver real-time situational awareness and insights for stations, tracks, and rolling stock, moving from reactive to precautionary and proactive interventions.

Autonomous Safety & Security

There will be a similar convergence of technologies into drones and robots, creating the ability to autonomously monitor, assess, detect and respond to threats or maintenance needs wherever they are, minimising human risk and improving response time.

Seamless, Immersive Connectivity

Emergence and adoption of 5G/6G and innovative deployment methods, such as by LEO satellite, will support uninterrupted communication between devices, systems, and operators — whether in remote or highly built-up areas.

Secure & Ethical Systems

Cybersecurity and privacy-preserving methods will evolve to ensure that the service and operational efficiencies which can result from smarter spaces are sustained by stronger cybersecurity and designed-in privacy preservation and ethics.

Human-Machine Collaboration

An evolution in human interfaces coupled with AI personalised assistance will empower staff to make faster, better-informed decisions while reducing their cognitive load.

A horizons-based model to scan for future tech

A *horizons-based framework* was utilised to scan for evolutions in technology with the potential to influence VSS solutions across the industry over the lifetime of the Strategy.

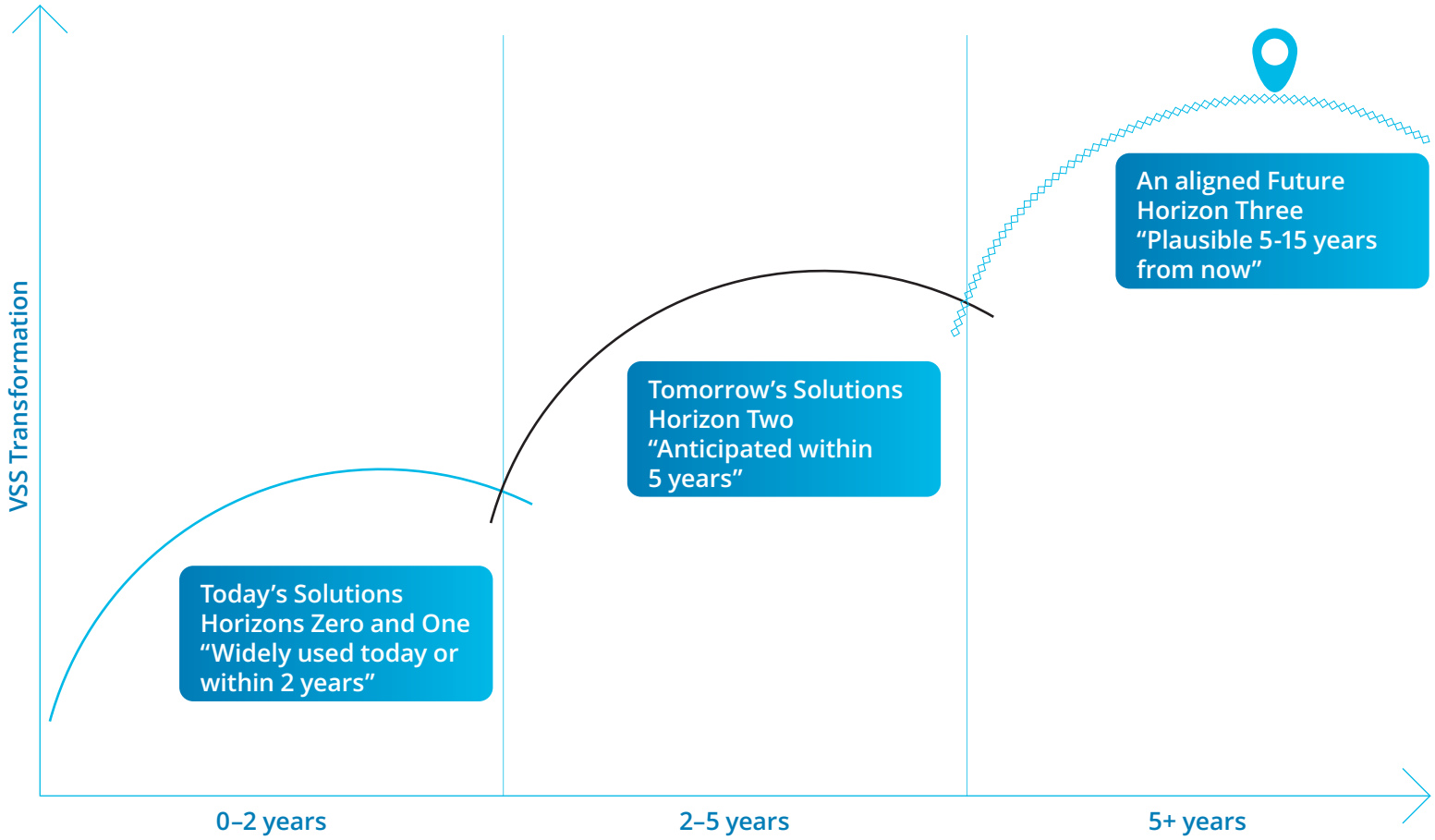
The scanning process has been tailored to be **both thought-provoking** and **grounded in reality,** recognising that adoption of new technologies can be constrained by **legacy infrastructure, fixed investment plans** and other factors such as **ethics** or **changing the nature of work.**

The scan aims to **reflect today, envision tomorrow** and support others to **build aligned perspectives,** bridging the gap, for example, recognising that full adoption of new technology may span **multiple control periods.**

Horizons Zero* and One explores **Today's Solutions** – those technologies which are already in widespread use or will be within two years.

Horizon Two explores **Tomorrow's Solutions** - those technology evolutions likely to be deployed widely within the next five years.

Horizon Three introduces more **stretch** to the scan, beginning to sketch an **Aligned Future** plausible between 5 and 15 years from now.



*Note that **Horizon Zero** reflects solutions typically in use across industries rather than specific deployment at Network Rail or across the rail industry.

Capsules of insight to stimulate debate and collaboration

A dynamic future technologies model has been developed to support collaborative engagement among VSS stakeholders, enabling the sharing of insights, trial planning, and the operationalisation of emerging solutions.

As technological advancement accelerates, the pace of change continues to increase. Inevitably, innovations will emerge and diverge in ways that may not be fully anticipated.

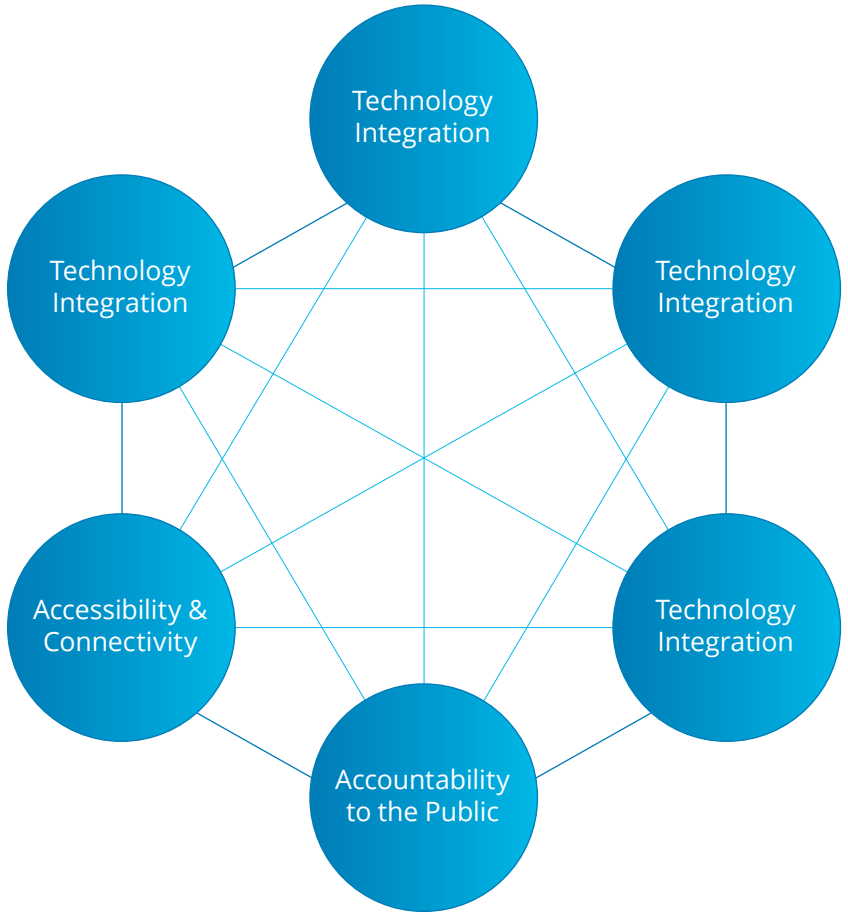
To navigate this evolving landscape, a capsule-based approach to insight has been adopted. Each capsule focuses on a key technology domain with significant potential to drive transformation in video surveillance over the Strategy's lifespan.

Alignment with the key Strategy Aspiration categories

- People Focus
- Technology Integration
- Rail Performance
- Accountability to the Public
- Accessibility & Connectivity

VSS Solutions & Hardware

VSS software solutions as typically deployed today.



Drone Solutions

Aerial and terrestrial drone solutions and the capabilities these can carry on board.

AI for Visual Intelligence

AI disciplines with particular relevance to Visual Intelligence (Machine Vision, Edge AI, Agentic AI and autonomy).

Connectivity

Non-traditional connectivity solutions *(i.e. beaming 5G / sat comms).*

Earth Observation

Satellite gathered terrestrial imaging and related analysis.

Cybersecurity

Identifying the tools and techniques needed to protect a diverse and evolving VSS estate.

Capsules Horizon Scan Overview

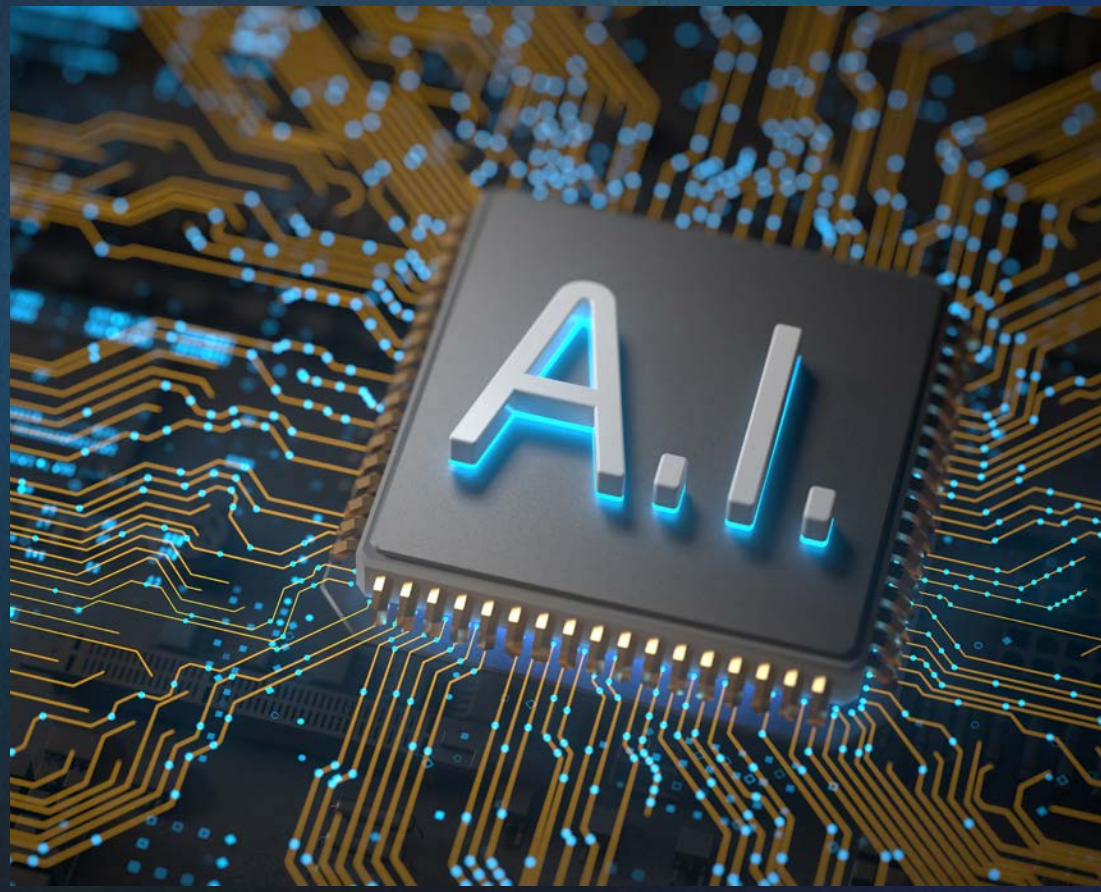
The future of VSS is not just about seeing more — it's about understanding more, acting faster, and doing so responsibly through the power of key technologies such as AI. There is a full supplementary report which provides further detail.

Capsule	Horizon 0 *(widely used today)*	Horizon 1 *(widely used within 2 years)*	Horizon 2 *(anticipated within 5 years)*	Horizon 3 *(plausible long-term future)*
VSS Hardware	**Systems:** Fixed/PTZ cameras, DVR/NVR, basic analytics, wired networks, locally managed software platforms. **Capabilities:** Basic situational awareness, manual post-event analysis, remote monitoring.	**Systems:** Edge AI cameras, 5G/Wi-Fi, satellite comms, hybrid cloud VSS, multi-sensor cameras. **Capabilities:** Real-time detection, predictive maintenance, intelligent alerts.	**Systems:** Modular platforms, digital twins, drones/robots with AI, low-power sensors. **Capabilities:** Proactive safety, asset tracking, human-machine collaboration.	**Systems:** Quantum analytics, bio-mimicking cameras, immersive displays, self-healing systems. **Capabilities:** Autonomous operations, personalized security, cognitive maintenance.
AI	**Systems:** Basic object, motion and incident detection, NPR and analytics. **Capabilities:** Intrusion detection, automated monitoring, basic tracking, vehicle access control.	**Systems:** Behavioural analysis, predictive maintenance, enhanced object detection. **Capabilities:** Proactive alerts, enhanced monitoring, passenger flow management.	**Systems:** Scenario simulation, anomaly detection across data streams, automated inspection. **Capabilities:** Predictive safety, automated reporting, and real-time risk assessment.	**Systems:** Cognitive video intelligence, federated learning, autonomous repair. **Capabilities:** Autonomous operations, immersive interfaces, adaptive systems.
Drones	**Systems:** Manual drones, GPS navigation, real-time streaming, basic inspections. **Capabilities:** Visual inspections, security patrols, incident response, vegetation monitoring.	**Systems:** Semi-autonomous drones, LiDAR, thermal imaging, edge processing. Capabilities: Automated inspections, thermal defect detection, autonomous security patrols.	**Systems:** Autonomous fleets, BVLOS drones, AI onboard analytics, hybrid power. **Capabilities:** AI reasoning, sensor fusion, collaborative autonomy.	**Systems:** Swarm drones, adaptive systems, micro-drones, energy harvesting. **Capabilities:** Cognitive inspection, proactive maintenance, autonomous railway integration.
Robotics	**Systems:** RC quadrupeds, UGVs, 3D sensors, robot mounted cameras. **Capabilities:** Infrastructure inspection, security patrols, incident response.	**Systems:** Tool-equipped robots, multi-robot communication, 5G, advanced robot mounted cameras. **Capabilities:** Automated inspections, thermal imaging, 3D modelling, autonomous security patrols.	**Systems:** Autonomous robots, robotic arms, docking stations, specialised forms. **Capabilities:** Predictive maintenance, precision monitoring, threat detection.	**Systems:** Swarm robotics, predictive repair, 24/7 patrols, autonomous alerts. **Capabilities:** Instantaneous repairs, autonomous alerts, self-monitoring systems.
Earth Observation	**Systems:** Medium-res imagery, GIS, manual interpretation. **Capabilities:** Environmental monitoring, post-event damage assessment, route planning.	**Systems:** High-res imagery, SAR, cloud platforms, automated change detection. **Capabilities:** Vegetation monitoring, landslide detection, hazard alerts, waterbody analysis.	**Systems:** EO + IoT integration, AI feature extraction, predictive analytics, 3D mapping. **Capabilities:** Real-time monitoring, threat detection, predictive maintenance.	**Systems:** Satellite tasking, EO + drone fusion, quantum EO analysis, digital twins. **Capabilities:** Autonomous alerts, predictive modelling, dynamic operations.
Advanced Connectivity	**Systems:** 4G/LTE, satellite broadband, local CCTV storage. **Capabilities:** Voice communications, basic data transfer, reactive investigation.	**Systems:** 5G NR, LEO satellite backhaul, hybrid satellite networks, real-time streaming. **Capabilities:** Enhanced remote diagnostics, anomaly detection, live monitoring, MCPTT and MCPTV support.	**Systems:** 5G-Advanced, FRMCS, edge computing, integrated LEO NTNs, drone/AGV comms. **Capabilities:** Collision avoidance, automated reporting, quantum cryptography.	**Systems:** 6G, terahertz comms, direct satellite-device links. **Capabilities:** Proactive risk mitigation, converged security systems, quantum-resilient comms.
Cybersecurity	**Systems:** Zero Trust infrastructure, AI/ML SOAR, quantum safe cryptography, resilient back-up, privacy-preserving technology. **Capabilities:** MFA, RBAC, workflow automation, hybrid cryptography.	**Systems:** SASE, NLP alert triage, advanced quantum safe cryptography, XDR. **Capabilities:** Real-time trust scoring, contextual enrichment, edge privacy analytics, ransomware kill-switch triggers.	**Systems:** AI trust brokers, PQC chipsets, passive diodes, homomorphic processors. **Capabilities:** Context-aware access, predictive containment, encrypted inference.	**Systems:** Adaptive trust fabrics, AI SOCs, QKD chips, privacy mesh. **Capabilities:** AI-defined access, full AI SOC coordination, autonomous cyber-hardening.

Footnote: *Please refer to the glossary on pages 103 for a detailed description of all the acronyms on this page.*

APPENDIX

3.3 IMPLEMENTING AI VSS MACHINE VISION

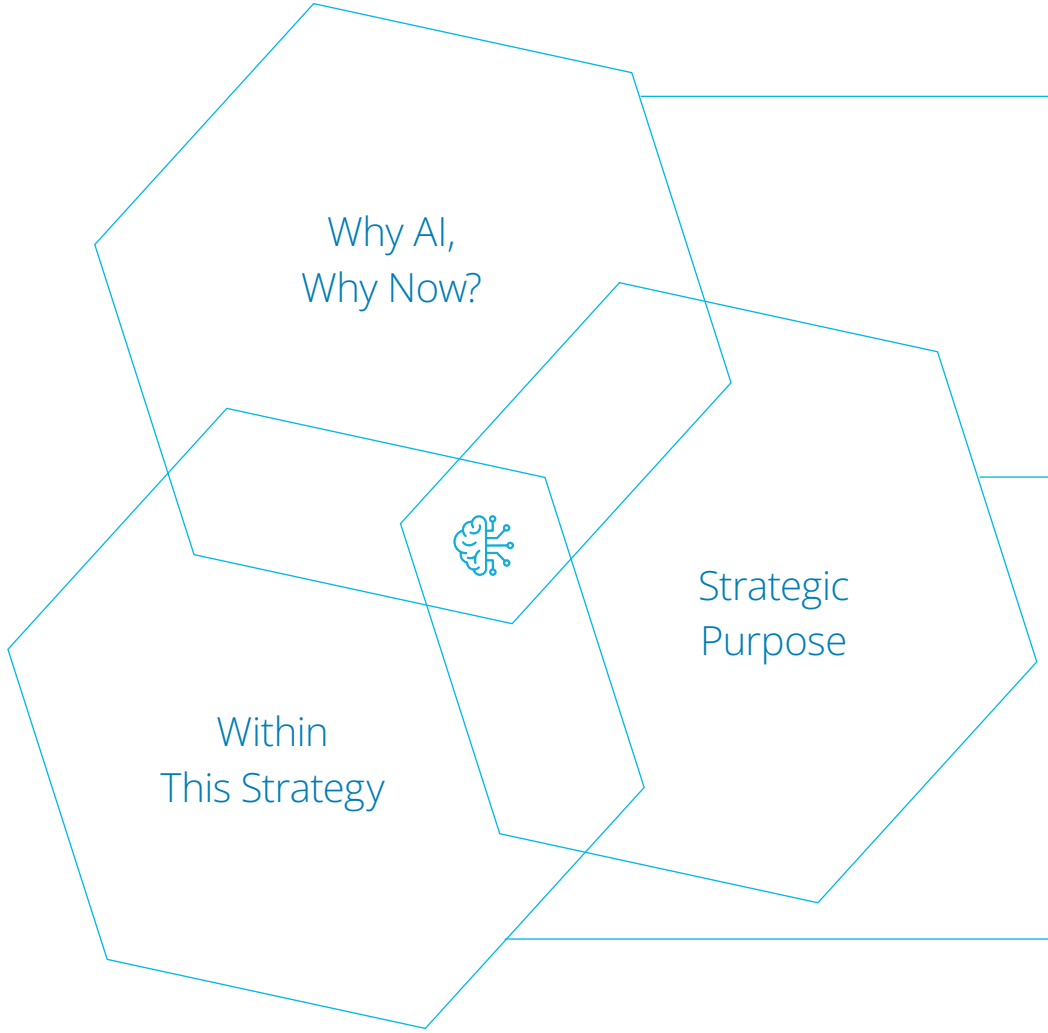


SECTION TAKEAWAYS:

The VSS AI Strategy provides a structured and actionable blueprint for deploying Artificial Intelligence across Visual Safety and Security use cases in the rail industry to enhance safety, security, and operational efficiency. NR DDaT or TOC equivalents should use this strategy to align fragmented initiatives, establish robust governance, and prioritise high-impact use cases... Foundational recommendations across operating model, governance, data, and culture highlight the importance of leadership, collaboration, and staff engagement in delivering a trusted, industry-wide VSS AI capability over the coming years.

AI Strategy Introduction

AI is an evolving technology which people want to exploit today and, in the future. This Strategy highlights some of the key considerations to enable effective deployment. There is a full supplementary report which provides further detail.



AI is a critical technological enabler that can help transform the rail industry from reactive visual safety & security to a proactive and intelligent model.

Current AI initiatives are fragmented, independently managed and lack central governance or strategic alignment.

To establish a unified, risk-aware and value-driven approach to AI deployment across the industry for VSS use cases.

Define best practices for AI procurement, development and deployment across the industry.

Ensure AI solutions are explainable, trusted and aligned to wider strategic goals.

What the VSS AI Operating Model could look like (using Network Rail as an example), with a focus on Strategy and governance.

Outlining the phases of the AI Development Lifecycle.

Setting out an AI Use Case Prioritisation Framework.

An AI Risk Assessment model to ensure the safe, ethical and compliant deployment of VSS AI.

Key Pillars for a VSS AI Operating Model

Initially designed for Network Rail, these are the three key pillars for the new VSS AI operating model that enables cross-industry engagement, alignment and collaboration.

VSS AI OPERATING MODEL

Hub & Spoke Model

In line with the industry AI Strategies, the model should involve an overall AI Hub made up of IT and technical approvers, with a smaller team (spoke) that is specific to the VSS space, which supports VSS AI initiatives and connects them with governance processes.

Focus on Strategy & Governance

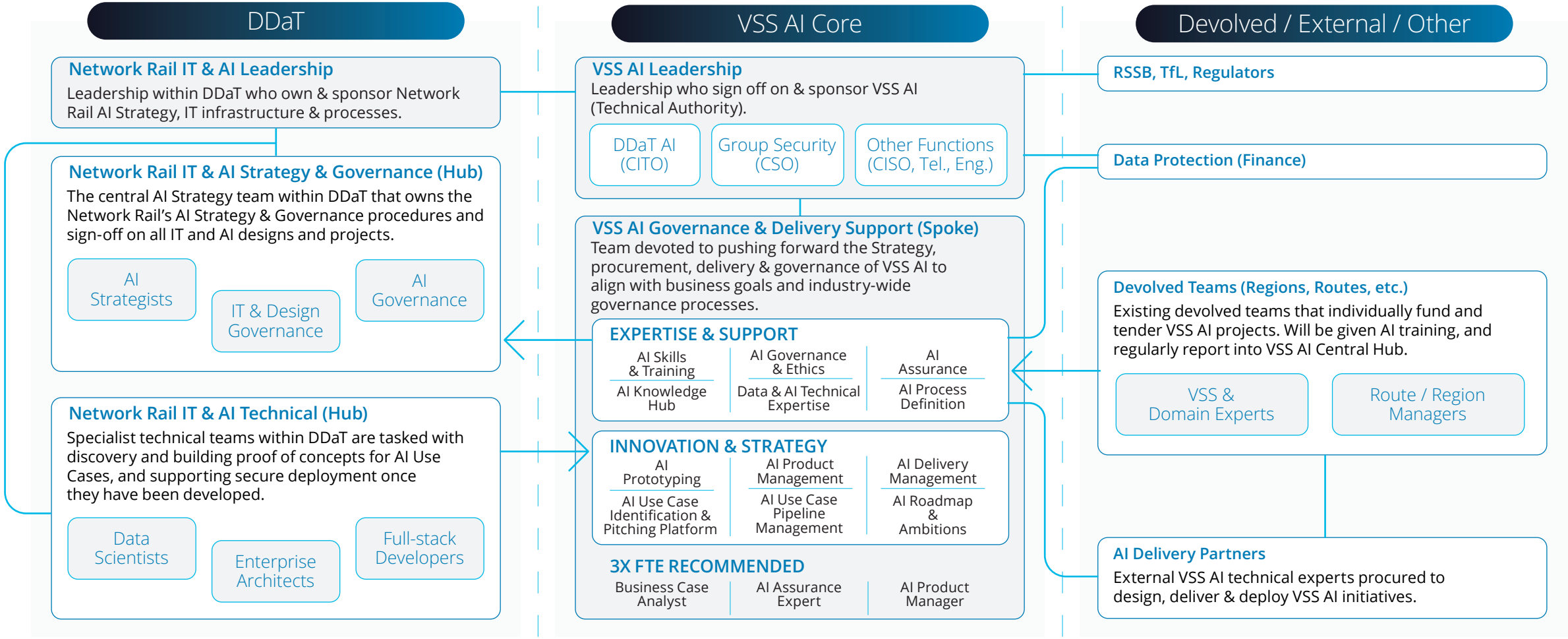
The key focus of the operating model is on Strategy & Governance, ensuring that all teams have clear visibility and oversight of VSS AI to ensure adherence to standards and alignment with industry-wide strategies.

AI & IT Approvals

The model must ensure that every VSS AI initiative must go through AI & IT governance processes and technical approvals, to ensure the security, suitability and viability from a technical perspective. Any governance and standards will be owned by AI & IT approvers and integrated into existing frameworks.

What Could a VSS AI Operating Model Look Like?

The hub and spoke model is designed initially as a Network Rail specific model that allows for engagement with the wider industry. However, this model also provides a path to evolve and be adopted across the industry in a post-GBR landscape. The example below shows the model in a Network Rail context in preparation for GBR:



Key Pillars For AI Governance

These are the three key pillars for VSS AI Governance. Together, they provide a structured approach to using AI safely and effectively, while ensuring that AI is deployed in line with strategic objectives.

VSS AI GOVERNANCE

Clear Alignment to Strategy & Business Value

VSS AI initiatives must clearly align with the wider industry Strategy and have a clear path to business value. To ensure this, a system must be put into place to measure the suitability of AI use cases from the outset of the AI Lifecycle.

Continuous Risk Assessment

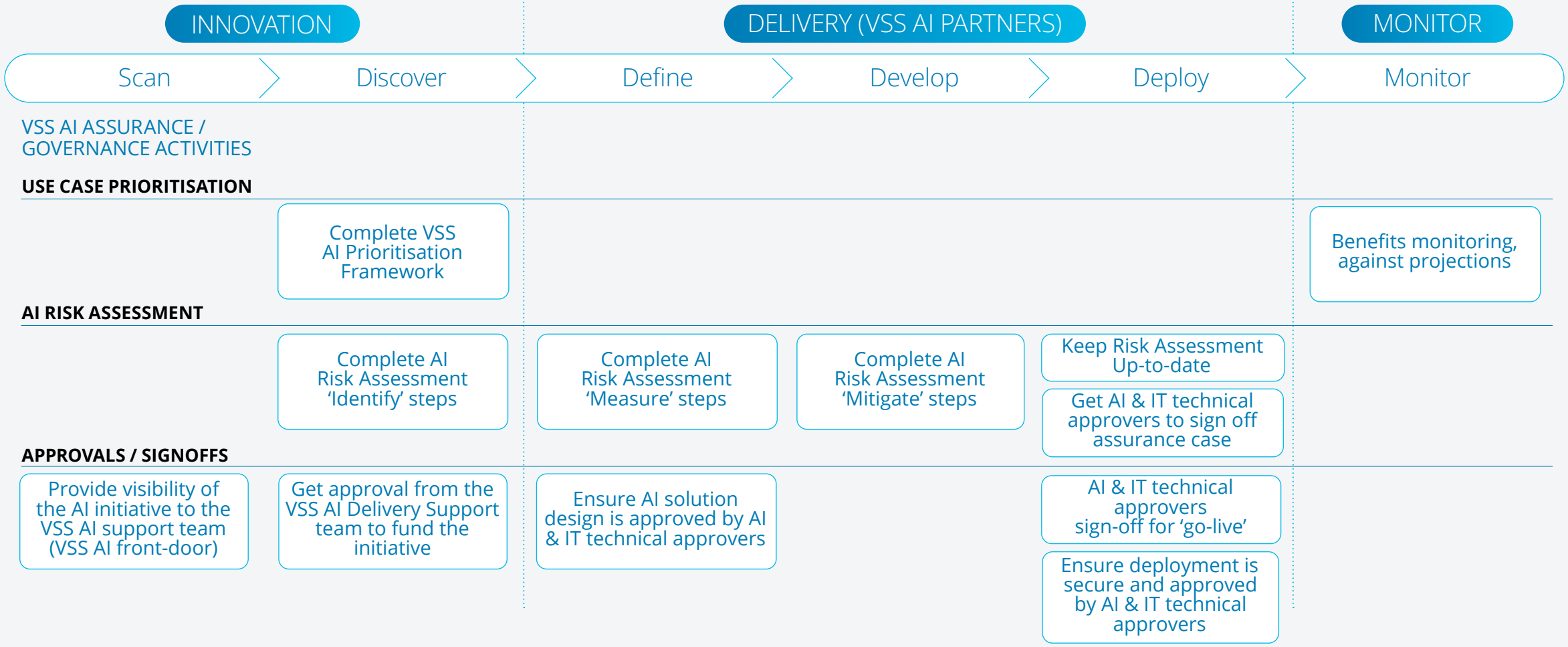
Given the wide range of potential risks to VSS AI initiatives, the governance processes must ensure that there is a risk assessment carried out from Day One, a clear process for measuring and mitigating risks, and the relevant support for filling out risk assessments throughout the AI Lifecycle.

Clear Process, Roles & Touchpoints

The governance processes must ensure that there is a clear definition of the AI Lifecycle, the roles at each stage (who delivers, supports and approves) and clear touchpoints with the AI & IT technical approvers to ensure adherence, in line with the existing Governance Guardrails.

Building The Governance Guardrails For VSS AI

For the industry to deploy AI more effectively, there needs to be guardrails which direct and refine the rollout of AI. The AI Assurance and Governance processes below have been designed so that key industry stakeholders, such as Network Rail, can work more effectively to manage potential AI deployments while simultaneously empowering them to meaningfully engage with industry suppliers regarding AI.



AI Use Case Prioritisation Critical Success Factors

To support the effective deployment of AI, a prioritised use case and risk assessment tool has been developed, which captures the themes noted below. Understanding the priorities and risks associated with AI will enable the entire industry to have collaborative conversations about how AI will be deployed, along with any opportunities, risks or interdependencies across stakeholders. All organisations should complete their own risk assessments for each AI use case they're looking at deploying, while also aiming to create their own AI use case prioritisation framework which aligns with both their organisational goals and wider industry priorities.

By scoring each category out of 5, a clear picture can be developed on whether the use case is viable *(potential to adjust weightings)*

AI Suitability

Is AI suitable for this use case, or could a more effective solution using traditional methods suffice?

Data, AI & Overall Solution Feasibility

Is there high-quality data readily available to train the models?

Is the solution technically feasible for our suppliers to build and will it be future-proof?

Alignment & Scale

Is the use case a priority category that aligns with strategic goals?

What regions will it effect? Is it only rolling out locally, or nationwide?

BENEFITS ALIGNMENT

Reduced Delays & Payouts

How big would the potential impact be on reducing delay costs?

SUCCESS METRICS

- Overall delay costs
- Delay costs attributed to delay types *(e.g. trespass, asset failure)*

Improved Safety & Security

How big could the potential benefit be in safety & security for passengers, the public, rail users and staff?

SUCCESS METRICS

- Number of incidents *(fatalities, level crossing injuries, etc.)*
- Reduced response times to incidents

Improved Perception of Safety

How much could this improve the public perception of safety on the railway?

SUCCESS METRICS

- RSSB survey outputs
- Sentiment of media coverage on railway safety

Integration with Existing Systems/Process

Is there a clear path to integration into the business process/system?

Will staff/users buy-in to the new AI technology and adopt the technology fully?

Is there a clear failsafe for situations where the AI isn't performing well?

Impacts on Staff

Will staff be upskilled in using the new technology? Is there a plan for this?

Will the technology lead to a loss of jobs, responsibilities or skills for staff?

Will it add workload for staff?

Use of Existing Infrastructure

Will this be using existing cameras or installed as part of a necessary VSS upgrade?

Would any new infrastructure installed be future-proofed and reusable in other initiatives?

Uses existing networks & storage?

Consistency with Other VSS AI Initiatives

Does this follow the guidance and best-practice that has been set?

Is it consistent with VSS AI initiatives in other areas across the industry?

Could these AI initiatives be linked together?

Timelines, Cost & Funding

How long will running a trial take and will it add value?

How long will full deployment take and how much will it cost?

Long-term funding & rollout, including long-term service cost (OpEx, storage, connection, etc.).

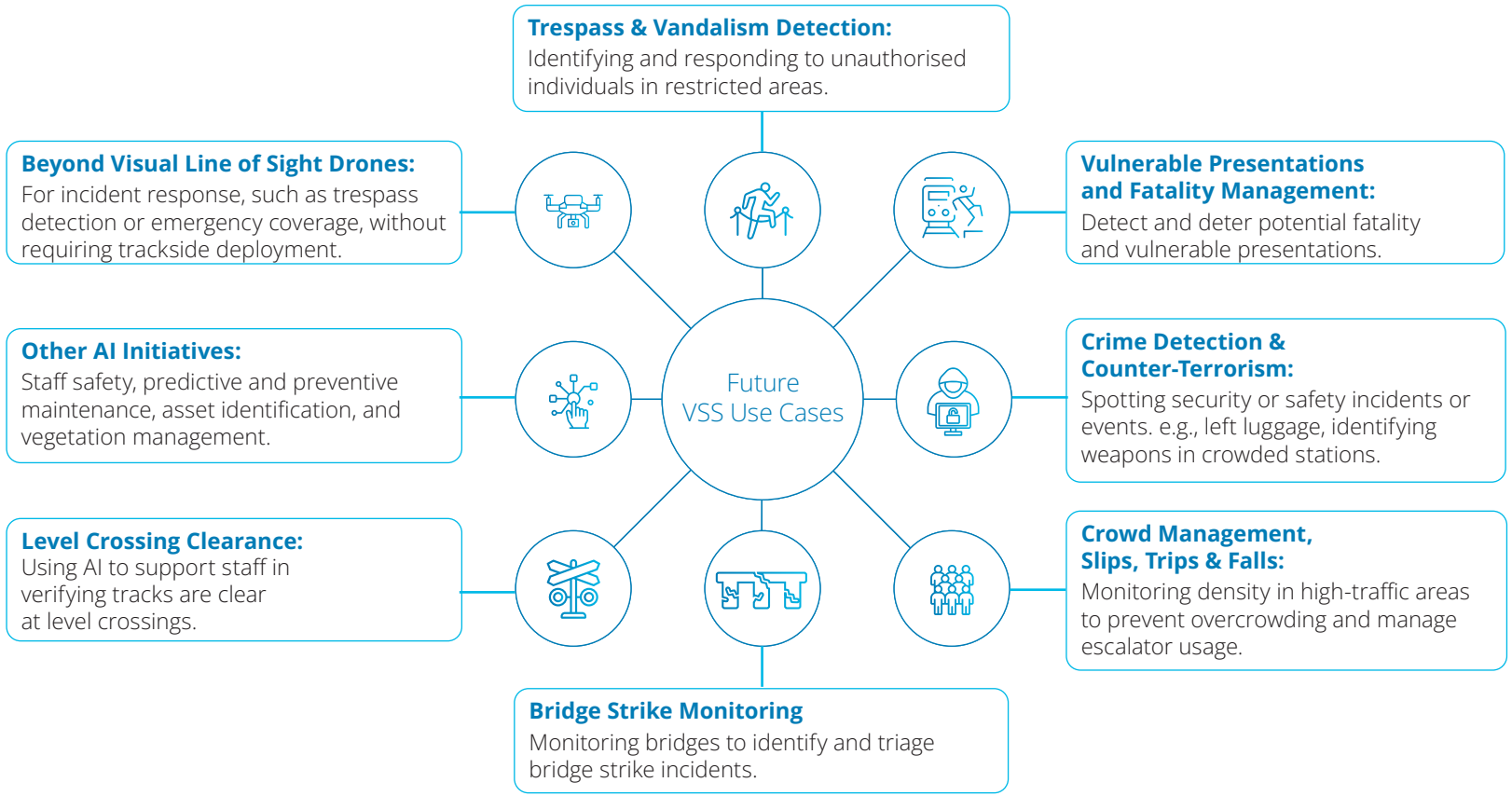
Risk Assessment

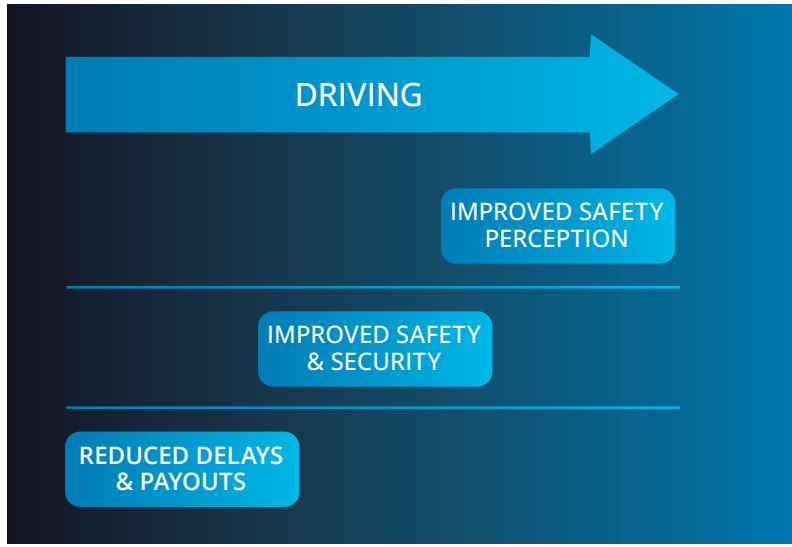
What is the output of the risk assessment?

How close is it to the risk tolerance threshold?

AI Use Case Category Shortlist

Using the prioritisation framework, a shortlist of **five use case areas** has been identified as potentially achievable through **VSS AI solutions** and can bring the **greatest benefit to the rail industry.**





Benefits & Associated Metrics for AI Initiatives

AI initiatives could potentially bring **3 key benefits** for the Rail industry:

Reduced Delay Minutes & Compensation Payouts

Improved timeliness of trains, leading to a reduction in the cost associated with delay.

SUCCESS METRICS

- Overall delay costs
- Delay costs attributed to delay types *(e.g. trespass, asset failure)*

Improved Safety

Improved safety for passengers, railway users and staff.

SUCCESS METRICS

- Number of incidents *(fatalities, level crossing injuries, etc.)*
- Reduced response times to incidents

Improved Perception of Safety

Improved public perception of safety on the railways, through confidence that VSS AI will keep them safe.

SUCCESS METRICS

- RSSB survey outputs
- Sentiment of media coverage on railway safety

POWERED BY

Pre-emptive Incident Flagging

AI can pre-emptively flag potential incidents to staff so they can be quickly identified or avoided.

Faster Reaction Post-Incident

AI can quickly identify and analyse key sections of incident footage, to allow for quicker post-event analysis so that action can be taken quickly.

More VSS Insights Generated

AI can identify insights that would have been missed by staff, to give more data on safety & security to feed into future Strategy.

Summary of recommendations from the Strategy

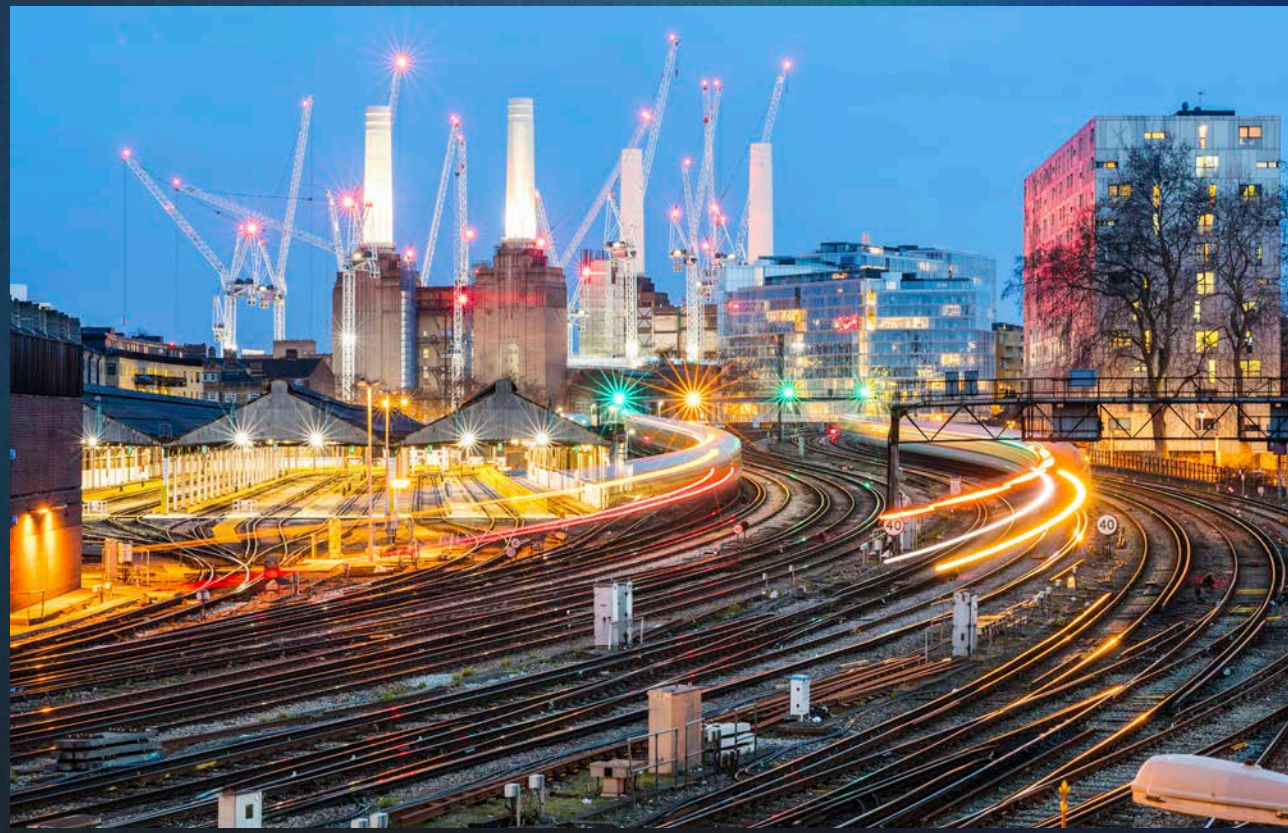
Foundation for VSS AI Strategy

Next Step for Implementation Phase of VSS AI Strategy

Operating Model	**Creation of an AI Strategy & Governance Hub,** to have visibility of all AI initiatives and oversight for a unified approach to AI Strategy & governance. The initial priority of this team is to get clear visibility of AI use and deployment across the industry for AI VSS initiatives.	**We recommend using a hub and spoke operating model,** where smaller teams within each area that use AI feed into the central technology function, e.g. DDaT for Network Rail, to ensure alignment and compliance with governance.	**Setting up a VSS AI Governance & Delivery Support Spoke team** to feed into the central technology function. This team will push forward the Strategy, procurement, delivery & governance of VSS AI. It will ensure that the devolved teams' funding and tendering VSS AI projects are aligned with business goals and industry-wide governance.	Once the 'AI Strategy & Governance' Hub & Spoke model is implemented, we recommend linking into the **Central Technology Function and IT & AI Technical approvers,** to create an **'AI Innovation Lab'** and **'AI Factory'** capability. This team is tasked with leading discovery, building proof of concepts for AI Use Cases, and supporting secure AI deployment once use cases have been fully developed.	**By creating a resilient operating model, we can ensure visibility of the wide range of VSS AI initiatives and a clear view of roles and responsibilities across the wide range of industry stakeholders involved in VSS AI.**
Governance	Creation of an AI governance framework with **clear processes, roles & touchpoints.** This includes a clear definition of the AI development lifecycle, the roles at each stage (who delivers, supports and approves) and clear touchpoints with the central technology function to ensure adherence. The new governance activities should be built within the existing Governance Guardrails framework.	**Ensure clear alignment of VSS AI to Strategic Goals & Business Value** by building a prioritisation framework into the governance processes to measure the suitability of AI use cases from the outset of the AI Lifecycle.	**Build and implement an AI Risk Assessment process.** Given the wide range of potential risks to VSS AI initiatives, the governance processes must ensure that there is a risk assessment activity from the outset of an AI initiative, a clear process for measuring and mitigating risks, and the relevant support for filling out risk assessments throughout the AI lifecycle.		**A strong governance framework will ensure standardisation and compliance of VSS AI initiatives across the industry while ensuring AI initiatives are value-generating and within accepted risk tolerances.**
Data & Technology	In line with the wider VSS technical Strategy, the AI Strategy supports the building of a **standardised model for the storage of VSS footage in a central, industry-owned cloud location,** which has AI compute capabilities for scalable industry-owned AI models.	To prove the capacity to develop AI solutions in-house, we recommend developing a **VSS AI Proof of Value** to validate that the infrastructure across the industry is capable of developing VSS AI and has a path to deploying it at scale.			**Data & Technology is the backbone of being able to create a scalable, industry-controlled VSS AI Strategy.**
Leadership, People & Culture	**Agree on clear sponsorship** of AI across the industry to build momentum and have accountability for AI at Network Rail, and industry-wide levels.	**Create a culture of visibility & collaboration** within VSS AI, so that devolved teams with shared goals or infrastructure work together to fund and build AI.	Ensuring that **staff** are consulted about AI solution design and **upskilled** in using the AI systems.		**VSS AI requires clear leadership, collaboration and upskilling of staff.**

APPENDIX

3.4 ECONOMIC ASSESSMENT



SECTION TAKEAWAYS: This early economic case sets out a strong strategic foundation and economic value, whilst highlighting the need for more granular data and structured evidence to inform any future investment cases.

Benefits Summary

This initial economic case sets out a strong foundation and provides a strategic industry benefits case. It can serve as the foundation for any further business cases that may need to be produced for national or regional VSS deployments.

Benefits

The benefits of VSS are mapped to five outcome areas:

- Safety
- Operational performance
- Staff and user experience
- Environmental sustainability
- Strategic resilience

While only a subset of benefits can currently be monetised (e.g. up to £20m annual savings in Schedule 8 delays, and £6–16m annual savings from reduced fatalities), these represent only part of the total value. The broader benefits include:

- Fewer incidents
- Stronger resilience
- Improved passenger confidence
- Smarter operations

Costs

Whilst the Strategy outlines VSS across various use cases, the cost analysis focuses on stations due to their high infrastructure demands, immediate strategic importance, and the greater availability of reliable cost and deployment data for stations. Costing for other use cases is expected to be developed as part of future business case enhancement.

Costs have been produced using previous VSS deployment projects at stations to form the baseline for indicative costs for this programme, but these costs vary widely depending on station maturity, especially fibre connectivity, with camera hardware typically representing only ~10% of the cost. The majority of spending is driven by enabling infrastructure, integration, and delivery overheads.

A scalable, scenario-based approach has been developed: targeting 'strategic compliance' at priority stations to unlock early safety and operational benefits, rather than deferring value for full optimisation.

Key cost drivers

The single largest cost driver is the installation of digital connectivity infrastructure at stations without existing capability.

Other material cost lines include design/assurance, delivery costs (incl. possessions), decommissioning of legacy systems, and integration with BTP platforms.

Recommendations and next steps

Embed upgrades into planned renewal cycles, standardise technical specifications, and confirm integration pathways with BTP.

Asset Owners to plan future VSS investments (e.g. Control Period or departmental funding applications) in line with recommended technical architecture.

Undertake station infrastructure maturity assessments to refine CapEx forecasts.

Map incident density hotspots to prioritise investment in high-impact areas.

Explore additional monetisation pathways for benefits, and pilot structured benefits tracking.

Where Strategic Ambition meets Practical Delivery: outlining what investment could look like, and why it matters for rail's evolution

The implementation of a modern Visual Safety & Security (VSS) System is a critical enabler for delivering a safer, more efficient, and more responsive railway. It enhances how the industry prevents and manages incidents, while supporting smarter, data-driven operations.

This chapter presents an early-stage view of the expected investment and potential benefits associated with implementing the VSS strategy.

The case is built around two key dimensions:

The benefits – at this stage, primarily qualitative – reflect the potential this capability unlocks for the rail industry.

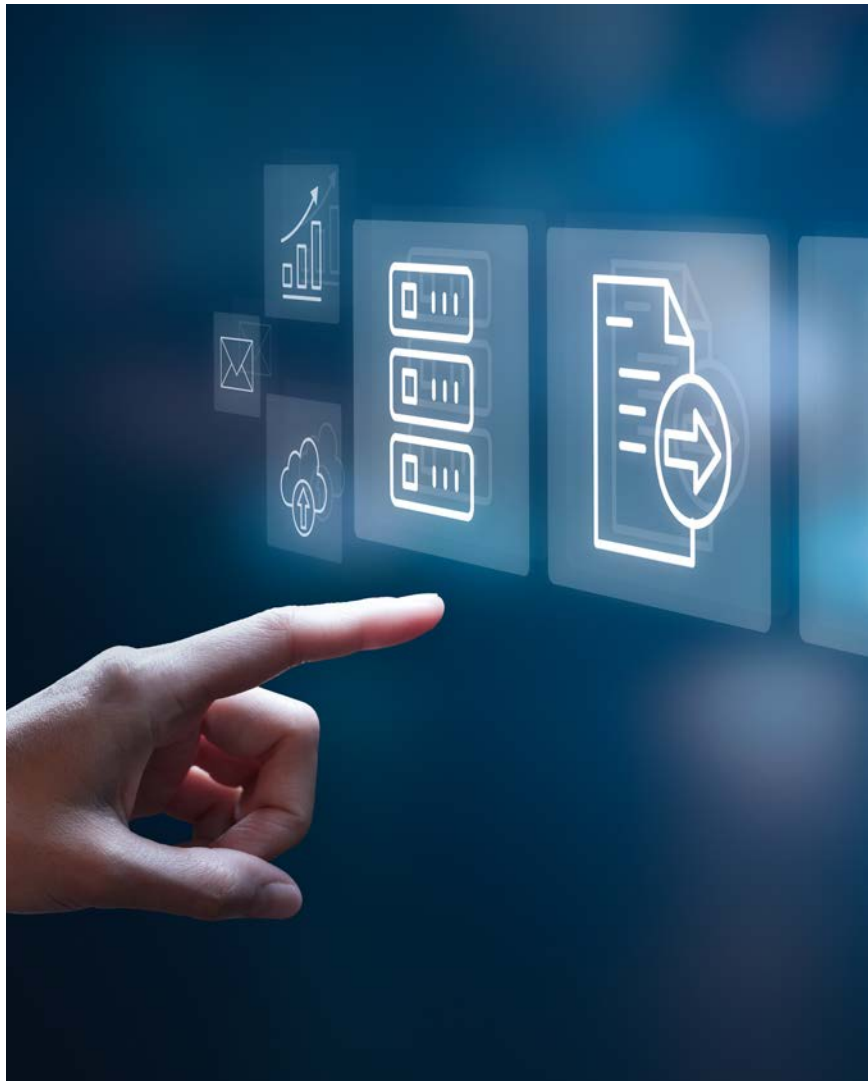
Monetised benefits are limited to areas where reliable data is available and reflect only a subset of the full investment case. A more detailed quantification – along with further validation – will be required to demonstrate the full impact of the strategy can bring.

The costs of delivering enhanced VSS capability across the network.

The strategy supports a scalable, scenario-based approach to implementation in order to unlock early operational and safety gains.

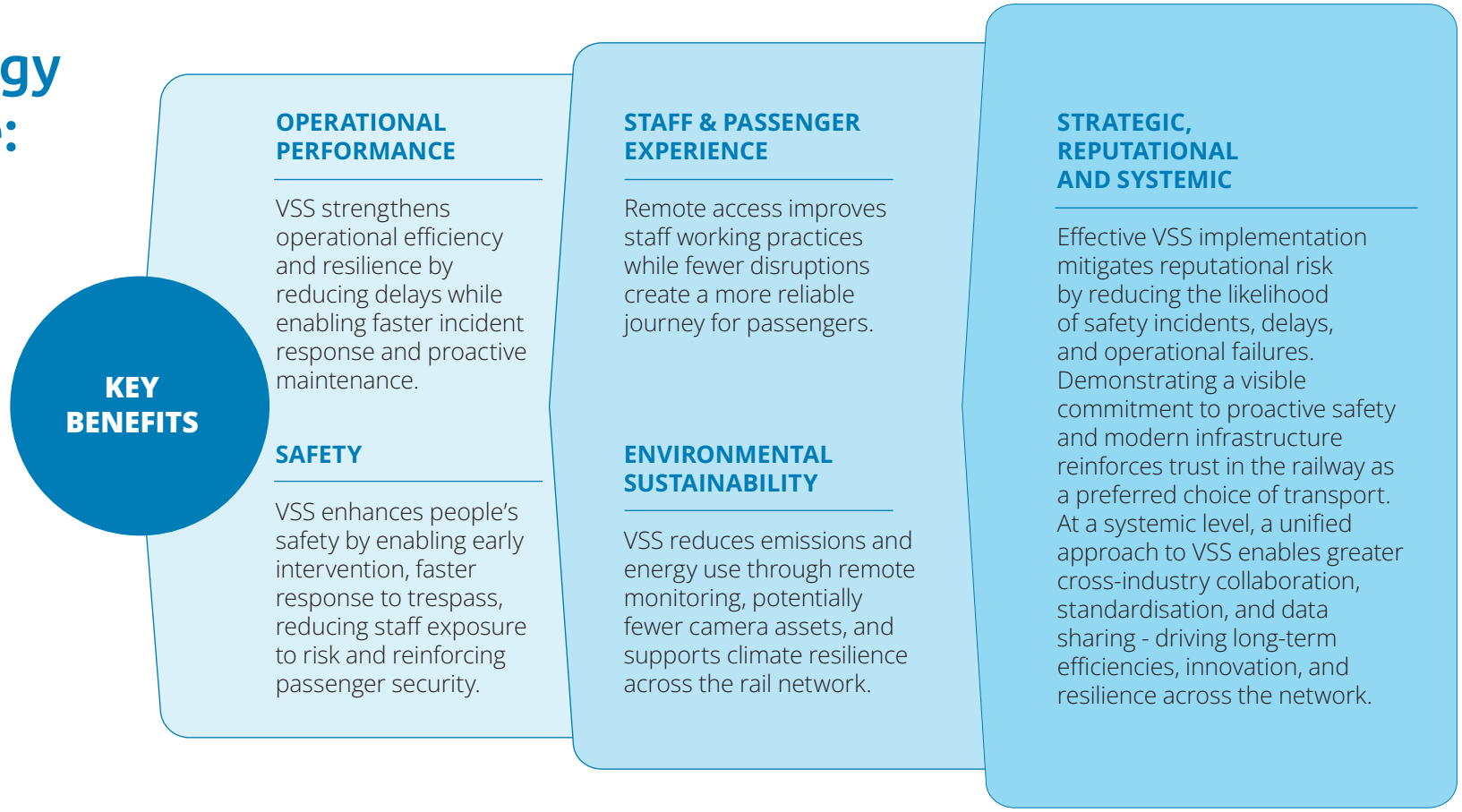
Though the ability to measure all figures precisely is complex, because of a lack of accurate and comprehensive data. The strategy takes a balanced approach. It indicates the full spectrum of benefits that VSS delivers and the associated investment required.

This analysis is intended to support decision-making, enabling industry leaders to engage in planning, prioritisation and investment with clarity and foresight.



At the core of this Strategy lies a clear value promise: *one that radiates wider benefits across the railway system.*

The benefits of the VSS Strategy are mapped to **five strategic outcome areas,** reflecting the wide-ranging impact the programme aims to deliver across the railway network. This section introduces these benefits in layers - from the most direct and measurable gains at the core, to the broader strategic outcomes that reinforce safety, resilience, passenger confidence, and long-term value for the industry.



Unlocking the Full Value of Safer, Smarter Stations

Why These Benefits Matter
Many of the most critical benefits of VSS are strategically aligned with the UK rail industry's national objectives and reflect areas of increasing priority. Whilst they remain difficult to quantify using current datasets, these outcomes represent high-value priorities for passengers, operators, and system leaders alike.

> We can have a fatality classified before officers even arrive on scene sometimes, because we have been able to remotely tap into the station CCTV and our commanders can review the footage which is clear and provides an overview of the incident itself, as well as the moments leading up to it" ***- BTP Central Disruption Unit Inspector***

Operational Performance
VSS enables more efficient, proactive, and resilient railway operations. Enhanced visibility through high-definition, networked cameras supports faster incident detection, response, and recovery - minimising delays and service disruptions.
The integration of intelligent analytics allows for predictive maintenance and early intervention, helping to prevent failures before they occur. These capabilities reduce operational overheads and enhance network availability, ultimately supporting more reliable, punctual service delivery across the rail estate.

£6.5m - £20m per annum

Estimated annual savings per annum, post Strategy implementation, in Schedule 8 costs, based on a 5-15% reduction in incident-related delays, enabled by improved VSS[1].

Staff and User Experience
Staff and user experience benefits stem from reduced disruption and greater operational flexibility enabled by VSS. For staff, remote monitoring reduces the need for travel to site, improving working conditions, efficiency, and morale. For passengers, fewer disruptions and faster recovery from incidents result in a more reliable and positive travel experience - strengthening overall confidence in the network.

Environmental Sustainability
VSS can enable remote diagnostics and monitoring, thereby lowering associated travel emissions and energy consumption. It also supports proactive maintenance and improves the network's ability to anticipate and respond to climate-related risks. Enhancing passenger experience through greater reliability and safety may also encourage a modal shift from more carbon-intensive forms of transport.

> *[On Forward Facing CCTV]* In the cases that we looked at, it saved an average 12 minutes of classification" ***- BTP Central Disruption Unit Inspector***

£6m – £16m per annum

Estimated annual savings per annum, post Strategy implementation, based on a 2% reduction in fatalities across the network enabled by improved VSS capabilities[2].

Safety
Advanced VSS capabilities play a critical role in protecting both passengers and staff simultaneously enhancing reputational benefits. Remote access and monitoring reduce the need for trackside inspections, lowering workforce exposure to hazardous environments. Real-time monitoring and analytics improve situational awareness, enabling quicker response to safety-critical events such as trespass, vandalism, or obstruction. For passengers, the presence of visible and responsive monitoring systems fosters a greater sense of security—reinforcing the railway as a safe and trusted mode of transport.

20%

Early analysis suggests that upgrading from analogue to digital/IP systems could yield up to a

20% annual reduction in OPEX[3].

What Drives Investment Today
While traditional business cases focus heavily on monetised returns, feedback from Network Rail's RTAPMs indicates that current VSS investment decisions are more strongly influenced by non-financial drivers (which may have an impact financially too), including:

1. **Risk reduction:** The development of business cases for installing new cameras have historically been informed by risk profiles, misuse history, and the potential for risk reduction.
2. **System obsolescence:** Replacing unsupported analogue infrastructure with scalable, interoperable alternatives to avoid maintainability and supportability issues that might otherwise arise.
3. **Strategic alignment:** Integrating with broader AI, control centre, and digital station initiatives.

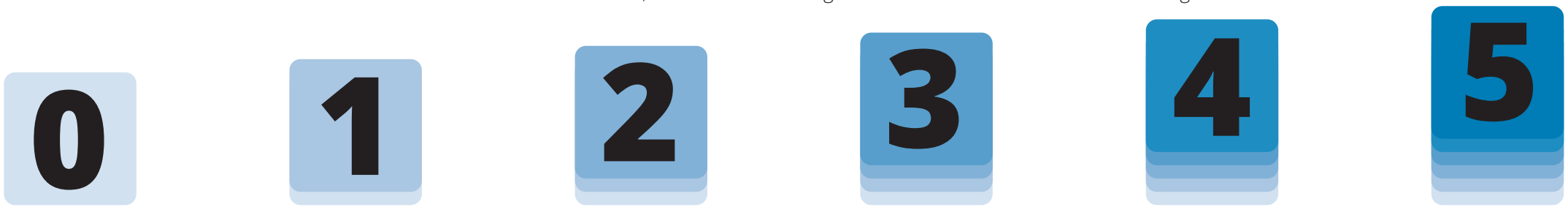
This Strategy therefore introduces a fit-for-purpose benefits model - one that reflects the full value case, not only benefits captured in monetary terms.

Footnotes: [1]Based on TRUST data collated from FY24/25. A total of 19,179 incidents at an average Schedule 8 cost of £6,755 per incident. [2]Based on data from FY24/25, which showed there were 317 fatalities, and the average value of prevention per casualty at £2,643,174. Source: DfT TAG Data Book, May 2025. [3]Based on a provisional estimate based on some high-level analysis on London-based stations.

Whilst the Strategy outlines VSS across various use cases, the cost analysis focuses on stations due to their high infrastructure demands, immediate strategic importance, and the greater availability of reliable cost and deployment data for stations. Costing for other use cases will be developed as part of future business case enhancement

Tailoring Investment to Infrastructure Maturity

This section outlines the indicative cost framework applied to different upgrade scenarios for stations within the Visual Safety & Security Systems (VSS) Strategy. Recognising the substantial variation in station infrastructure maturity across the network, the model reflects the differing levels of investment required to bring each site up to a strategically compliant standard. It is also noted that there may be maturity scenarios for other use cases across the rail network, such as level crossings and on-board train systems. Costs vary significantly depending on baseline conditions - most notably, the presence of fibre connectivity. While camera hardware typically represents a small share of the total cost, the enabling infrastructure (e.g. power, fibre) often drives the majority of capital expenditure and requires site-specific planning. A breakdown of cost assumptions by scenario is included in the Appendix, highlighting the most material cost lines relevant to the modelling.



SCENARIO 00

Business As Usual

Business-as-usual approach. Infrastructure is maintained in line with existing policy and legislative requirements only.

Regular renewals of legacy CCTV equipment take place in line with renewal cycles, but no strategic upgrades or capability enhancements are introduced.

SCENARIO 01

Partial Upgrade 1

Enhances system bandwidth only. Intended for stations where network constraints are the primary limitation to VSS performance. No physical equipment upgrades; intervention focuses on network performance improvements.

SCENARIO 02

Partial Upgrade 2

A light-touch digital enablement. Involves limited infrastructure work, such as adding switches/nodes and enabling unused software features already present in the system. Intended for sites that have recently undergone hardware upgrades and require minor upgrades to unlock full system functionality.

SCENARIO 03

Partial Upgrade 3

Focuses on expanding surveillance coverage by adding new HD IP cameras to an already modernised or recently upgraded infrastructure. No backbone or remote access upgrades, but it ensures infrastructure can support additional cameras. Most of the benefit comes from hardware enhancements only.

SCENARIO 04

Partial Upgrade 4

A hybrid upgrade approach that retains some existing infrastructure while delivering core system upgrades. Involves installation of new NVRs, new Cloud-Based VSS and control equipment, and new UPS systems. Does not replace the fibre backbone or install new cameras, but provides significant system improvements.

SCENARIO 05

Full Refresh

A comprehensive end-to-end replacement of the CCTV infrastructure. Includes new HD IP cameras, full fibre backbone replacement, new switches and nodes, new Cloud-Based VSS/ control equipment, backhaul installation, new UPS, and upgrades to support analytics. Represents the highest level of investment and capability.

Targeted investment begins with a clear picture of what drives cost and where it delivers the biggest impact

This cost model underpins the economic case for delivering the Strategy across the rail network. It is grounded in prioritising upgrades at stations that will deliver the greatest immediate value, rather than deferring benefits in pursuit of full optimisation from day one. Data suggests that just two regions are responsible for a disproportionately large share of delay minutes across the network, with the highest-delay regions accounting for approximately 59% of total Schedule 8 delay costs[1]. As such, the model supports a staged approach - focusing initially on enabling 'strategic compliance' across priority stations to unlock early operational and safety gains, waiting to deploy only when all components are fully matured would defer benefits and risk value for money. The cost projections presented here are high-level and indicative. They are designed to support strategic planning and investment discussions, recognising that precise figures will depend on local asset condition, procurement route, and integration complexity at individual sites.

Capital Expenditure (CapEx)[2]

A full breakdown is included in the Appendix 10.

This model only includes the most material CapEx costs required to bring a station up to strategic compliance with the VSS Strategy. Specifically, it includes 1. Fibre infrastructure (nodes and edge switches), 2. Cloud infrastructure, 3. Distributed Control Centre System, 4. Connectivity, 5. Training & Change Management and 6. Legacy System decommissioning). It excludes 1. Routine renewal costs, which fall under business-as-usual (BAU) renewals and therefore should not be attributed to the VSS Strategy (e.g., cameras, UPS, installation, cabling, power), 2. Strategic "bolt-ons" not yet fully defined (e.g., AI analytics, cloud hosting, distributed control systems) and 3. Any site-specific enhancements are not essential for strategic compliance.

Station Category *(further details available in Appendix 10)*	**Estimated CapEx cost by year, for all stations per Category of station**					
	FY25/26	**FY26/27**	**FY27/28**	**FY28/29**	**FY29/30**	**FY30/31**
A	£ 11,700,000					
B		£ 14,900,000				
C			£ 27,500,000			
D				£ 16,500,000		
E					£ 18,900,000	
F						£ 33,400,000
GDP Deflator Index[3]	£12,000,000	£15,150,000	£28,000,000	£16,900,000	£19,200,000	£34,700,000
Technology Price Erosion (8%)[4]	£11,000,000	£13,900,000	£25,900,000	£15,500,000	£17,700,000	£31,900,000
Cumulative Total CapEx	£11,000,000	£24,900,000	£50,800,000	£66,300,000	£84,000,000	**£115,900,000**

Operational Expenditure (OpEx)

Early indicative analysis suggests that upgrading from analogue to digital/IP systems could yield up to **20% reduction in OpEx.** This estimate is based on a provisional estimate based on high-level analysis of London-based stations. Key sources of savings include reduced frequency of engineer site visits, avoidance of maintaining obsolete or unsupported systems and improved reliability and fewer service interruptions.

Footnotes: [1]Network Rail Trust data FY2024/5 [2]CapEx Modelling Assumptions: Estimated CapEx per platform at £27,804, Implementation Year: FY2025/26, Base Year: FY2024/25. The CapEx figure was derived using cost data from a recent station upgrade project, which was a full delivery across a 7-platform station and 50% delivery at a 6-platform station. Given these were large, London-based stations with unique access challenges and extensive legacy system decommissioning, a 40% cost reduction was applied to reflect a more typical regional station. The resulting figure was then normalised per platform. [3]Inflation Adjustment: In line with HM Treasury guidance, GDP deflators are applied annually. For years beyond FY2029/30, a flat deflator of 2% per annum is assumed (FY25/26 102.65, FY26/27 101.66, FY27/28 102.04, FY28/29 101.95, FY29/30 101.88, and FY30/31 103.88). [4]Technology Price Erosion: Based on technical consultation, core hardware costs (cameras, servers, storage) are assumed to decline by 7–8% annually due to market efficiencies and innovation cycles.

Lifting the Lid on What Drives Cost in VSS Implementation

A clear understanding of the cost drivers behind Strategy implementation is critical to ensuring realistic planning and efficient allocation of funding. While hardware procurement is a relatively small proportion of total costs, the infrastructure and integration required to support modern, scalable systems present more material cost lines.

Connectivity-Led Costs

The single most material cost driver is the installation of connectivity infrastructure at stations lacking modern digital capability.

This includes fibre backhaul, edge switching, integration layers and local networks required for remote access and live analytics.

These works are inherently site-specific and often require complex engineering interventions, particularly in limited-access environments.

Weightings of costs

Hardware - such as IP cameras, recording systems, and supporting equipment - typically accounts for just 10% of overall project costs.

The remaining 90% is concentrated in supporting infrastructure and delivery, including:

- Design and assurance.
- Delivery and contractor costs *(incl. possessions costs).*
- Legacy system decommissioning.

Enablers of Cost Efficiency

Long-term value for money will depend on:

Aligning with planned renewals: Embedding VSS upgrades into existing capital renewal cycles.

Standardising technical specifications: Promoting consistency across suppliers and delivery partners to reduce duplication and accelerate deployment.

Integration Costs: There may be increased integration costs during the transition period for legacy and third-party architecture.

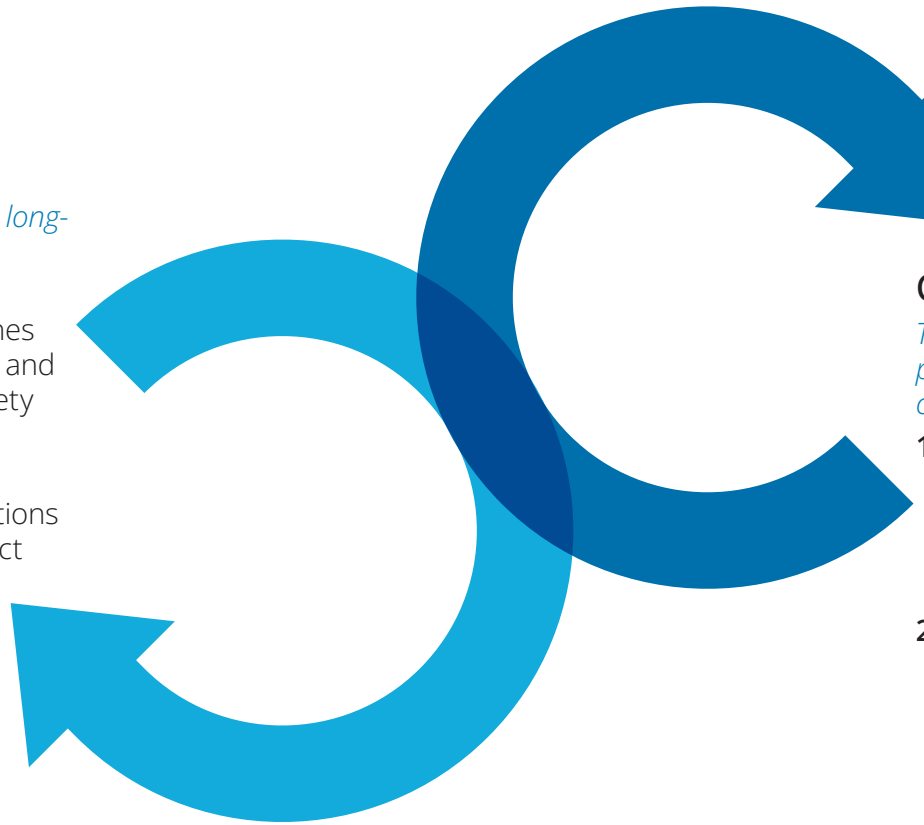
Turning Vision into Delivery requires focused Investment Insight

While this Strategy provides a directionally strong foundation, further work is required to unlock a more detailed and specific investment case. The following activities are recommended to strengthen both the cost and benefits case in subsequent phases of business case development:

Enhancing the Benefits Case

Although qualitative benefits are clear, structured evidence is required to support monetisation and long-term performance tracking:

1. **Explore further monetisation pathways**
   Develop proxy-based or empirical approaches to link VSS functionality with cost avoidance and performance uplift (e.g. reduced delays, safety interventions), quantified where possible.
2. **Pilot Structured Benefits Tracking**
   Implement benefits tracking at selected stations to measure pre-/post-implementation impact across safety, security and performance dimensions.



Cost Refinement Priorities

To move from network-wide assumptions to station-specific planning, further granularity is needed on infrastructure conditions and implementation environments:

1. **Undertake a Station Infrastructure Maturity Assessment**
   Identify existing capabilities (e.g. fibre, power, camera coverage) at each station to tailor CapEx estimates more accurately.
2. **Map Incident Density Hotspots**
   Overlay incident data (e.g. trespass, safety events) with station infrastructure maturity to prioritise high-impact intervention areas.

APPENDIX

3.5 RAID

SECTION TAKEAWAYS:

This section on the Context and Vision have been developed from the inputs of industry SMEs and major rail stakeholders.

The VSS Strategy starts by presenting its purpose. The VSS Vision is then defined with its supporting strategic objectives, which outline the direction and priorities for enhancing safety, security and performance across the network. Ensuring that the Strategy implementation delivers meaningful, measurable impact.

APPENDIX **VISION STATEMENT AND STRATEGIC OBJECTIVES**

Turning Vision into Value: Unlocking the Full Potential of VSS

Strategic Objectives

The Strategic Objectives outlined in this Strategy define the direction and priorities for **enhancing safety, security and performance across the network.**

They are designed to align with broader industry-wide goals and to guide investment decisions for any organisation – regardless of their current maturity – seeking to implement or enhance VSS in line with best practice.

ASPIRATIONS

PEOPLE FOCUS

- Developing the capabilities and trust to accelerate the adoption of technology.
- Train and support staff skillset to be scalable and flexible to change.
- Ensure passengers, the public and railway users feel safe and secure when interacting with the railway.
- Remove fragmentation and barriers across industry with a unified approach.

ACCOUNTABILITY TO THE PUBLIC

- Transparent and lawful use of personal data and people's liberties.
- Provide a clear explanation for when and how AI is used in the decision-making process.
- Inform and consult the public of any major changes to security systems where necessary.
- Everything that is delivered is compliant with GDPR, protects personal data and stays ahead of regulatory changes.
- Use visual intelligence for a safer and more secure railway.
- Enhance cybersecurity and data protection.

ACCESSIBILITY & CONNECTIVITY

- Enable National Rail, TOCs, FOCs and BTP to securely access live and recorded video data, analytics, and system health insights through a unified and resilient infrastructure.
- Ensure end to end systems and asset locations are well connected and interoperable.

TECHNOLOGY INTEGRATION

- Be consistent in the deployment of innovative technology and asset quality.
- Adopt common principles and ensure implementation of best practices.
- Innovate and harness the potential of technology & AI.
- Ensuring technology meets open source principles and has long-term maintainability.
- Use camera renewals and upgrade opportunities to switch from analogue to IP or AI-enabled.

RAIL PERFORMANCE

- Maximise measurable value to performance, safety and people.
- Strengthen the analytics and data management capabilities.
- Stopping incidents proactively and recovering from incidents quickly rather than responding to them reactively.

APPENDIX 1 Risk Log Guidance

FIELD	DEFINITION
PROBABILITY	Likelihood/Probability that the risk will become an issue is defined as follows: 5 – more than 70% (almost certain) 4 – 50-70% (fairly likely to occur) 3 – 30-50% (possible it may occur) 2 – 10-30% (less likely) 1 – less than 10% (remote) 0 – Risk is no longer a threat - i.e. fully mitigated
IMPACT	Impact should the risk become an issue is defined as follows: 5 – High Impact - Critical impact on the overall achievement of objective and overall performance. Critical impact on costs and/ or reputation. Very difficult and possible long term to recover 4 – Medium / High Impact - Major impact on costs and objectives. Serious impact on output and /or quality. Medium to long term effect and expensive to recover 3 – Medium Impact - Significant waste of time and resources. Impact on operational efficiency, output and quality. Medium term effect which may be expensive to recover 2 – Low / Medium Impact - Minor loss, delay, inconvenience or interruption. Short to medium term effect 1 – Low Impact - Minimal loss, delay inconvenience or interruption. Can be easily and quickly remedied.
OVERALL SCORE (IMPACT x PROBABILITY)	The Overall Score is calculated by multiplying the Impact score by the Probability score. This results in a score between 0 (fully mitigated risk) and 25 (severe and highly likely risk). This score provides a numerical indication of the severity of the risk and informs prioritisation (see below).
PRIORITY	20-25 Critical – Highest priority risks that could significantly derail delivery objectives. Requires immediate and sustained action. 15-19 High – Major risks that need to be addressed and actively managed in the short term. 10-14 Moderate – Medium-level risks that require planning but can be managed within existing controls. 0-9 Low – Lower-level risks with limited impact or low probability. Monitor periodically

APPENDIX **2** Full Risk Log 1/2

ID	DESCRIPTION	MITIGATION	RISK SCORE			PRIORITY
			IMPACT SCORE	**PROBABILITY SCORE**	**OVERALL SCORE** *(IMPACT vs PROBABILITY)*	
R1	**FUNDING** Securing funding for asset renewals and enhancements could be a challenge, as the industry is constrained regarding the current funding position for CP7, which may lead to delays or compromises in project scope.	Develop a VSS business case highlighting the long-term benefits and cost savings of the project to secure necessary funding from stakeholders and potential investors. Develop a renewal-based Capability Roadmap which is flexible allowing capability growth as and when funding is available. Looking at alternatively funding models/ servitisation to reduce cost may also help mitigate this.	**5**	**4**	**20**	**CRITICAL**
R2	**STRATEGY COMPLIANCE** There has been difficulty in the past aligning Network Rail regarding agreed architectural principles & patterns and doing this across the whole industry will be a challenge as the vast range of stakeholders all have separate sets of requirements, making it a challenge to piece these together.	Utilise VSS Steering group and VSS Task & Finish Groups to ensure regular communication and collaboration amongst industry stakeholders. Develop the Strategy in collaboration with industry stakeholders to ensure it meets the needs and expectations of all parties involved.	**5**	**3**	**15**	**HIGH**
R3	**CYBERSECURITY COMPLIANCE** Network Rail will need to comply with various Cyber Security policies. According to lessons learned from other projects, these requirements could be quite onerous and difficult to adhere to, therefore this could be costly to implement, or the project may need to find alternative solutions.	Cybersecurity compliance requirements are to be reviewed, documented and integrated into architectural design principles. Continuous review of alignment to cybersecurity principles with key industry stakeholders.	**5**	**3**	**15**	**HIGH**
R4	**PEOPLE CHANGE MANAGEMENT** If change management is not done well in terms of skills, capability, and resources, it will cause problems during the implementation of the Strategy, leading to delays, increased costs, and potential failure to achieve strategic objectives.	Implement phased adoption of Strategy in change management approach and include lessons learned learnt from previous work that has not gained traction/ has faced resistance (London Bridge AI trial). Developing a comprehensive change management plan with training, capability assessments, and adequate resource allocation should be developed and regularly monitored.	**5**	**3**	**15**	**HIGH**
R5	**LEGAL COMPLIANCE** There are many data protection and legal policies applicable to VSS systems and VSS AI capabilities which presents a compliance challenge. Any new systems deployed must adhere to these policies to avoid the risk of non-compliance, which could result in severe penalties, legal actions, and reputational damage due to violations of government security data protection regulations.	Develop and implement a robust compliance framework that aligns with industry standards around data protection, and encourage adherence to these standards during the deployment of new systems	**5**	**3**	**15**	**HIGH**

APPENDIX 3 Full Risk Log 2/2

ID	DESCRIPTION	MITIGATION	RISK SCORE			PRIORITY
			IMPACT SCORE	PROBABILITY SCORE	OVERALL SCORE *(IMPACT vs. PROBABILITY)*	
R6	**DATA PROTECTION & ETHICS** There is a risk that an increased number of users having access to VSS footage could result in unethical misuse or data breaches. This can be caused by expanded access across multiple stakeholders without adequate governance, audit, or control mechanisms. This may impact data protection compliance, trust, and could result in reputational damage or regulatory scrutiny.	Implement a robust access control framework that includes user role-based permissions, audit logging (including purpose of access), and regular access reviews. Establish clear governance policies outlining who can access VSS footage, under what circumstances, and with what level of authorisation. Embed data protection impact assessments (DPIAs) in any expansion of access rights. Provide mandatory training for all users on data privacy, legal obligations, and ethical handling of footage.	5	3	15	HIGH
R7	**LEGACY SYSTEMS** The extensive presence of legacy systems within the VSS infrastructure increases the risk for integrating newer architectural solutions. This may result in substantial upgrades being required, increasing both the cost and complexity of the technical solution.	Develop a flexible phased approach to upgrade legacy systems gradually, reducing immediate financial burden and allowing for smoother integration with newer architectures.	3	4	12	MODERATE
R8	**PUBLIC TRUST** There is a risk that the public may misunderstand or mistrust the use of VSS technologies due to lack of clear communication on privacy and safety measures.	Develop a public engagement and comms plan for the implementation phase of the Strategy	3	4	12	MODERATE
R9	**UNION BUY IN** Getting union buy-in for the VSS Strategy and future AI implementations could be a challenge, which could delay or hinder the implementation of the Strategy.	Engage with union representatives early in the process to address their concerns and involve them in the planning and decision-making stages.	3	3	9	MODERATE
R10	**MOMENTUM** Sustaining momentum with VSS strategic initiatives is challenging, and there is a risk of losing momentum over time, which could lead to incomplete or stalled projects.	Utilising VSS Task & Finish group to monitor progress, maintain momentum, and ensure continuous engagement from all stakeholders.	4	2	8	MODERATE
R11	**VSS IMPROVEMENT MORALE** Fatigue from historical attempts in the past to implement similar strategies have failed, leading to low morale and a lack of enthusiasm and support for new initiatives.	Communicate the lessons learned from past failures and outline a clear, achievable plan with milestones to rebuild confidence and morale among the team.	3	2	6	LOW

APPENDIX 4 Dependencies Log Guidance

FIELD	DEFINITION
PRIORITY	**Critical** - Essential external or internal input without which the Strategy or key milestones cannot progress. Requires committed delivery and regular tracking. **High** - Important dependency with material impact on timelines or outcomes. Should be actively monitored. **Moderate** - Medium-impact dependency that could delay or affect quality if not met, but manageable within delivery tolerances. Requires periodic check-ins. **Low** - Minor dependency with low likelihood of impact. Monitor through standard governance processes.

APPENDIX **5** Full Dependencies Log

ID	DESCRIPTION	DEPENDENT ON	ACTION	OWNER	PRIORITY
D1	**EXTERNAL STAKEHOLDER BUY IN** Dependency on the rail industry stakeholders to drive the implementation and technical changes of the VSS Strategy to enable VSS improvements across the rail industry.	Rail Industry-wide Stakeholders	As part of Strategy development, establish a Steering Group and engage with Task & Finish Groups. Conduct 1:1 interviews with key industry stakeholders to secure alignment.		**CRITICAL**
D2	**EFFECTIVE STRATEGY DELIVERY & IMPLEMENTATION HANDOVER** Dependency on Network Rail's DDaT function, and any similar functions within TOCs and FOCs, to act as the primary delivery owners for Strategy implementation.	NR, DDAT	Successful transition from Strategy development to implementation relies on early and sustained engagement with DDaT. Clear implementation governance structure proposed as part of the Strategy to maintain delivery momentum beyond development. Ensure DDaT and Technical Authority have a defined role in governance post-Strategy.		**CRITICAL**
D3	**TRADE UNION BUY IN** Dependency on trade union engagement to support AI implementations and avoid potential barriers to adoption.	Trade Unions	Early engagement with Trades Union to build understanding and address concerns around AI use, develop joint engagement plan to secure support to deliver a safer railway	NR Comms	**HIGH**

APPENDIX 6 Constraints Log Guidance

FIELD	DEFINITION
PRIORITY	**Critical** - Fundamental constraint that will severely limit scope, timing, or deliverability unless proactively resolved or adapted around. Requires immediate escalation or resolution Strategy. **High** - Major constraint with significant implications for the programme if not addressed. Needs to be actively managed with mitigation and contingency planning. **Moderate** - Constraint that may limit delivery flexibility or require changes to scope or sequencing. Manageable with ongoing monitoring and adjustments. **Low** - Minor constraint with minimal impact. Requires awareness but unlikely to affect overall delivery. Monitor and manage as part of standard project controls.

APPENDIX 7 Full Constraints Log

ID	CATEGORY	DESCRIPTION	IMPACT ON STRATEGY	ACTION	OWNER	PRIORITY
R1	**Time & Cost**	**FUNDING UNCERTAINTY & PRIORITISATION** The Strategy implementation is constrained by capital investment windows tied to Control Periods (CP7, CP8); differing budget processes across entities.	Limits flexibility in delivery timing. Strategy must align with financial planning cycles.	Phased implementation aligned to financial and digital maturity. Use the Business Case to support prioritisation in capital allocation. Maintain proactive engagement with DfT, ORR, GBR Transition Team, and other funders to influence forward planning and secure early commitment. Ensure the Strategy is synchronised with CP8 and future funding windows to maximise alignment with Network Rail and GBR investment plans.	RTAPMs/ GBR/TOCs	CRITICAL
R2	**Resource**	**STAFF ENGAGEMENT, UPSKILLING & RESOURCING** Front line staff must understand and adopt new video technologies to support the delivery of VSS Strategy with a sufficient resourcing model to support technology upgrades	Constrains safety, security and operational effectiveness	Develop a clear change management plan. Provide targeted training on AI/VSS usage, interpretation of outputs, and escalation procedures to build confidence. Training to be built into funding case as an ongoing requirement beyond initial deployment.	DDAT/TA	HIGH
R3	**Technical**	**CONNECTIVITY** The Strategy implementation is constrained by inconsistent connectivity coverage across stations and locations, which affects the reliability and performance of video technologies.	Increases the complexity and cost of deploying consistent VSS capabilities, potentially limiting operational effectiveness and user experience.	Implement the phased deployment approach that prioritises locations with sufficient connectivity. Leverage available infrastructure to demonstrate early value, while building the business case for broader investment. Include connectivity upgrades as part of long-term planning and funding alignment.	RTAPMs/ GBR/TOCs	HIGH
R4	**Technical**	**LEGACY INFRASTRUCTURE** The Strategy implementation is constrained by varying levels of system maturity, from analogue to digital, presenting integration challenges with existing platforms.	Increases complexity and cost of standardising and deploying unified solutions.	Phased rollout based on system readiness and integration standards, and the roadmap considers varying digital maturity. Integration standards are proposed to support legacy-to-digital transitions.	RTAPMs/ GBR/TOCs	MODERATE

APPENDIX 8 Opportunities Log Guidance

FIELD	DEFINITION
PRIORITY	**Transformational** - Significant opportunity with transformative potential to positively impact Strategy outcomes, scope, or cost-effectiveness. Should be actively pursued immediately. **High** - Major opportunity with substantial benefits for achieving strategic objectives. Requires proactive exploration. **Moderate** - Opportunity that offers meaningful enhancements or efficiencies if realised. Worth regular review and consideration for Strategy implementation. **Low** - Smaller-scale or longer-term opportunity with incremental benefits. Monitor and review for future consideration.

APPENDIX 9 Full Constraints Log

ID	DESCRIPTION	BENEFIT	PRIORITY
OP1	The Strategy presents an opportunity to position VSS as a national infrastructure priority, helping unlock government innovation grants and green technology funding.	Reduces dependency on traditional funding cycles, accelerates implementation, and attracts investment.	TRANSFORMATIONAL
OP2	There is an opportunity to enhance the Strategy business case by demonstrating long-term savings and improvements in safety, security, and performance, making it attractive to both public and private stakeholders.	Enhances the case for investment by demonstrating tangible value, increases likelihood of securing funding by being a key part of planning for future funding cycles.	TRANSFORMATIONAL
OP3	The Strategy presents an opportunity to develop connected systems that provide BTP and relevant Local Authorities with live access to critical feeds, enhancing situational awareness.	Enables faster incident response, improves situational awareness, which in turn helps reduce service disruptions and their associated costs. Supports a more proactive and coordinated approach to safety and security across the rail network.	TRANSFORMATIONAL
OP4	The Strategy presents an opportunity to align with and support the future GBR operating model by promoting consistency and interoperability in security infrastructure.	Helps industry partners transition effectively into GBR, reducing fragmentation and ensuring VSS systems are ready for integration into a unified rail governance model.	TRANSFORMATIONAL
OP5	The Strategy presents an opportunity to provide a common framework and shared standards, enabling more efficient and joined-up VSS delivery across the network.	Reduces duplication, improves interoperability, and accelerates implementation through consistent guidance and governance and working towards creating a more unified approach.	HIGH
OP6	The Strategy presents an opportunity to adopt a modular, phased approach to integrate cloud-native components with legacy platforms, while also piloting AI-driven analytics and predictive maintenance.	Enables gradual modernisation with minimal disruption, improves scalability, and unlocks data-driven operational efficiencies.	HIGH
OP7	The Strategy presents an opportunity to build a more robust and quantifiable benefits case for future projects and programmes as part of the implementation phase.	Improves investment confidence among key decision-makers such as DfT, supporting future business case approvals and funding allocations.	HIGH
OP8	The Strategy presents an opportunity to design a "Smart VSS" operating model that integrates process, governance, and technology dimensions for more intelligent operations.	Provides a clear capability roadmap for implementing future VSS, improving coordination across routes/region and driving an increase in rail performance. Products are also likely to be developed to a higher standard, and increased consistency.	HIGH
OP9	The Strategy presents an opportunity to optimise the use of physical assets, such as cameras, by enabling more intelligent and planned coverage, reducing the number of devices required.	Reduces up-front capital expenditure as part of implementation and then continuous operational expenditure by minimising redundant hardware, lowering maintenance costs, and decreasing energy consumption.	HIGH
OP10	The Strategy presents an opportunity to implement an AI and machine vision training curriculum tailored to different persona groups, supporting capability uplift across the organisation.	Builds targeted capability across the organisation, ensuring staff are equipped to work with emerging technologies such as, drones and agentic AI. This also establishes staff buy-in and familiarity with AI, supporting long-term digital maturity.	MODERATE

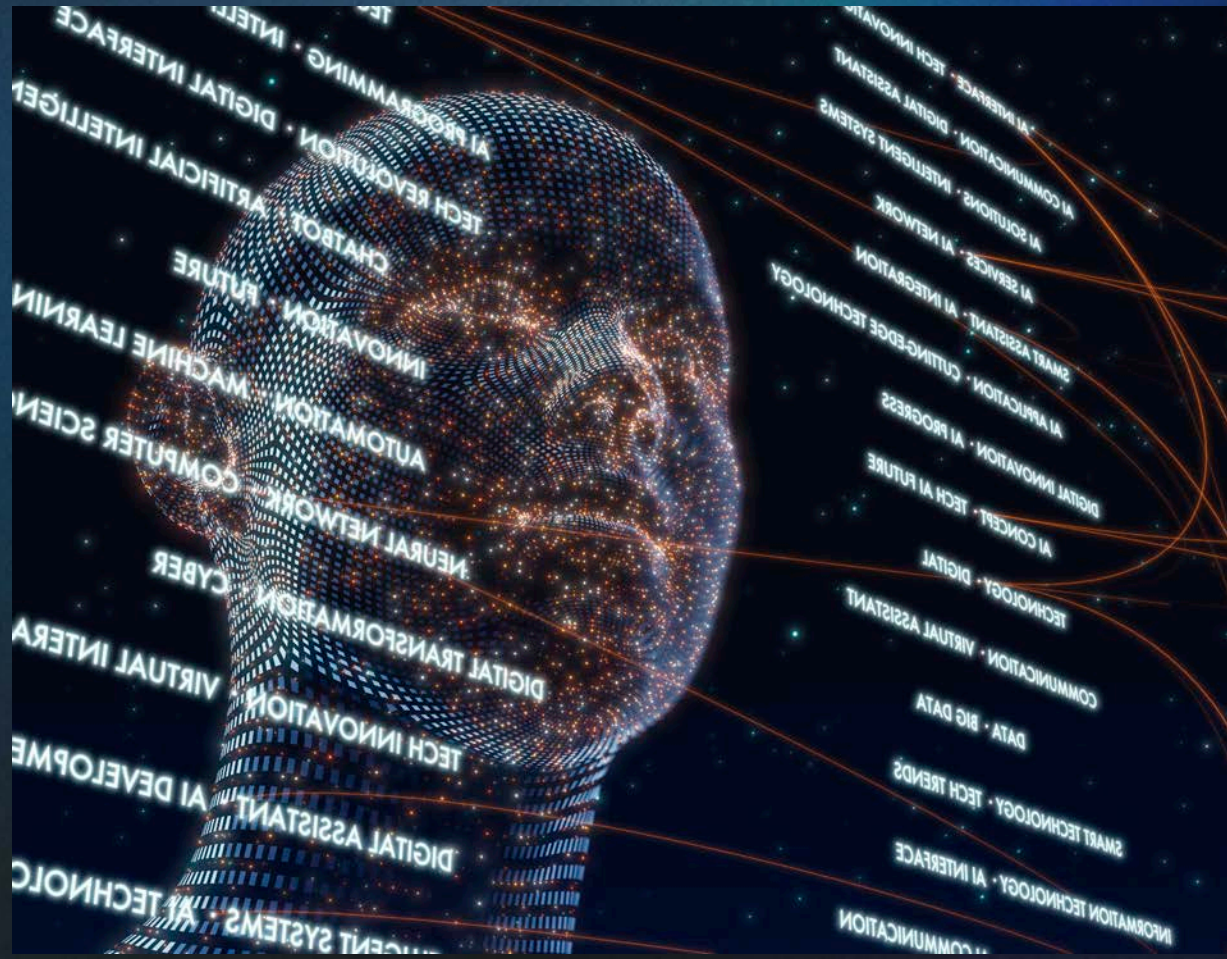
APPENDIX **10** Station Categories

The 2,597 railway stations on the National Rail network in Great Britain are classified into six categories by the Department for Transport.

Category	Journeys Made	Description	Example	Revenue Generated
A	28	National Hub	Birmingham New Street, London King's Cross	Over 2m trips: over £20m
B	67	Regional Interchange	Guildford, Nottingham	Over 2m trips: over £20m
C	248	Important Feeder	Grantham, Plymouth	0.5–2m trips: £2–20m
D	298	Medium Staffed	Abergavenny, Penrith	0.25–0.5m trips: £1–2m
E	695	Small Staffed	Deal, Oakham	Under 0.25m trips: Under £1m
F	1200	Small Unstaffed	Beccles, Bishop Auckland	Under 0.25m trips: Under £1m

3.6

GLOSSARY


AI PROGRAMMING · INTERFACE
TECH REVOLUTION · DIGITAL INTERFACE
CHATBOT · ARTIFICIAL INTELLIGEN
INNOVATION · FUTURE
AUTOMATION · MACHINE LEARNIN
NEURAL NETWORK · COMPUTER SCIEN
DIGITAL TRANSFORMATION · CYBER
TECH INNOVATION · VIRTUAL INTERA
DIGITAL ASSISTANT · AI DEVELOPME
SYSTEMS · AI TECHNOLO
AI INTERFACE · TECH INNOVATION
AI COMMUNICATION · DIGITAL ASSISTANT
AI SOLUTIONS · INTELLIGENT SYSTEMS
AI SERVICES · AI NETWORK
SMART ASSISTANT · AI INTEGRATION
AI APPLICATION · CUTTING-EDGE TECHNOLOGY
DIGITAL INNOVATION · AI PROGRESS
AI CONCEPT · TECH AI FUTURE
TECHNOLOGY · DIGITAL
COMMUNICATION · VIRTUAL ASSISTANT
DATA · BIG DATA
SMART TECHNOLOGY · TECH TRENDS
INFORMATION TECHNOLOGY · AI INTERFACE
COMMUNICATION

Glossary

A

AAD Azure Active Directory Microsoft's cloud-based identity and access management service that helps organisations securely manage user access to applications and resources across cloud & on-prem environments.

ACLs Access Control Lists A set of rules that specify which users or systems are allowed or denied access to resources such as files, networks or devices, helping to enforce security policies.

AES-256 Advanced Encryption Standard (with 256-bit key length) A highly secure symmetric encryption algorithm that uses a 256-bit key length to transform data into an unreadable format through rounds of complex substitutions and permutations.

ALARP As Low As Reasonably Practicable A risk management principle that requires reducing risks to the lowest level achievable, balancing the cost, time, and effort of risk reduction to ensure that further risk reduction is not grossly disproportionate to the improvement achieved.

ANPR Automatic Number Plate Recognition A technology using cameras and optical character recognition to automatically read and convert number plates into machine-readable data for law enforcement purposes.

API Application Programming Interface A set of rules and protocols that allows different software applications to communicate with each other.

ARK Access Risk Knowledge The understanding and awareness of the risks associated with unauthorised system access, including how access can be exploited and how to mitigate against these risks.

B

BAU Business As Usual The ongoing, routine operations and activities of an organisation that are necessary to maintain its normal functioning.

BMS Building Management System A computer-based control system that monitors and manages a building's mechanical, electrical and safety systems.

BTP British Transport Police Law enforcement agency responsible for policing Britain's railways; relies on VSS footage for crime prevention and investigation.

BVLOS Beyond Visual Line of Sight The drone pilot flies the drone beyond their direct visual range, relying on technology to navigate and monitor the drone.

BWV/BWC Body Worn Video/Camera Cameras that are small, visible devices attached to an officer's uniform, used to capture video and audio evidence during incidents

C

CAD Computer-Aided Design The use of software to create, modify, analyse or optimise 2D or 3D digital models or drawings of real-world objects.

CAPEX Capital Expenditure The money an organisation spends to acquire, upgrade or maintain long-term physical assets which are expected to provide value or benefits over multiple years.

CCTV Closed Circuit Television A VSS system that uses cameras to transmit video signals to a specific set of monitors or recording devices.

CIS Cybersecurity Information Security The practice of protecting computer systems, networks, and data from digital attacks, unauthorised access and damage.

CNI Critical National Infrastructure The essential infrastructure whose loss or compromise would cause significant disruptions to vital UK services.

CP Control Period A fixed five-year period used by Network Rail for financial planning, investment prioritisation and setting operational and maintenance targets for the railway infrastructure. Each control period begins on April 1 and ends on March 31 five years later.

D

DDaT Digital Data and Technology The division of Network Rail focused on leveraging digital technologies, data analytics and IT innovation to transform the railway's network operations.

DfT Department for Transport Govt. department responsible for the English transport network, including oversight of Network Rail's operations.

DOO Driver Only Operated Specialised type of VSS systems that provide real-time, low-latency live video feeds of the train platform interface to the driver's cab enabling drivers to safely monitor boarding.

DORI Detection, Observation, Recognition and Identification The four levels of visual detail used to evaluate camera performance, based on pixel density standards to match surveillance needs.

DPIA Data Protection Impact Assessment A process designed to identify and mitigate risks associated with the processing of personal data, ensuring compliance with data protection laws

DPO Data Protection Officer A person responsible for ensuring an organisation's compliance with data protection laws, monitoring data processing activities, and advising on data privacy matters

DR Disaster Recovery The process and set of procedures an organisation uses to restore IT systems, data and operations quickly after a disruptive event such as system failure or cyberattack.

DVR Digital Video Recorders A device that records and processes video footage from analogue cameras, converting it to digital format for storage.

E

EIP External Identity Provider A service that manages and authenticates user identities from outside an organisation, allowing secure access to its applications and resources

F

FOCs Freight Operating Companies Use VSS systems to monitor cargo security during transit.

FTNx Fixed Telecoms Network Extended A high-capacity optical telecoms network to support IP-based services and data-hungry applications, providing a secure and resilient backbone for communications and operations.

FTTC Fibre To The Cabinet A broadband technology where fibre optic cables deliver high-speed internet to a local street cabinet.

FTTP Fibre To The Premises A broadband technology where fibre optic cables run directly from the local internet exchange to a business, providing ultra-fast and consistent internet speeds.

FW Firewall A network security device or software that monitors and controls incoming and outgoing network traffic based on predetermined security rules, blocking unauthorised access and protecting the internal network from threats.

G

GBR Great British Rail A planned state-owned railway company that will manage the UK's rail infrastructure and passenger services.

GDPR General Data Protection Regulation A piece of legislation that governs the processing, protection and rights relating to personal data in the UK, supplemented by the Data Protection Act 2018 and regulated by the ICO.

GIS Geographic Information System A computer-based tool that captures, stores, analyses and visualises geographically referenced data.

GSM-R Global Systems for Mobile Communications - Railway An integrated digital wireless communications standard specifically designed for railway operations, enabling secure, real-time voice and data communications between train drivers, railway staff and control centres.

H

HO Home Office The lead government department for immigration, security, and law and order, which may use surveillance data from Network Rail to enhance public safety.

HR/IDM Human Resources & Identity Management Systems that centrally manage and automate the collection, storage, and processing of employee data and human resources processes.

Glossary

I

ICO Information Commissioner's Office The UK's independent body that upholds information rights in the public interest.

IoT Internet of Things A network of physical objects embedded with sensors, software, and connectivity technologies that enable them to collect, exchange, and act on data.

IP Internet Protocol A set of rules and standards that govern how data packets are addressed, routed, and transmitted across networks from a source device to the correct destination on IP-based networks or on the internet.

ITIL Information Technology Infrastructure Library A widely adopted framework of best practices designed to help organisations align their IT services with business needs, improve service management & enhance efficiency.

J

JSON JavaScript Object Notation A lightweight text-based data format that is easy for humans to read and write and easy for machines to parse and generate, used for transmitting data between a server and a web applications.

K

KPI Key Performance Indicator A quantifiable measure used to evaluate how effectively an individual, team, or organisation is achieving specific objectives.

L

LAN Local Area Network A network of interconnected computers and devices within a limited, localised area enabling communication and resource sharing among those devices.

LEO Low Earth Orbit (satellite networks) Satellites that orbit the Earth at altitudes between 200 to 2,000 km, providing low-latency, high-speed communications and global coverage through large constellations designed to enable reliable internet and data services.

LTE Long-Term Evolution A wireless broadband communication standard that significantly increases data speeds and network capacity for mobile devices.

M

MCB Manually Controlled Barriers Level crossing barriers operated by a signaller to fully close off the railway corridor, ensuring safe passage for trains and vehicles

MFA Multi-Factor Authentication A security process that requires users to provide two or more distinct forms of verification to confirm their identity and gain access to a system.

MNO Mobile Network Operator A telecoms company that owns or controls the infrastructure and licenses needed to provide services directly to mobile devices within a specific geographic area.

MPLS Multiprotocol Label Switching A network routing technique that directs data packets using short path labels, enabling faster and more efficient traffic flow across complex wide-area networks.

MVP Minimum Viable Product The simplest version of a product with just enough features to attract early users and gather validated feedback for future development and improvement.

N

NLP Natural Language Processing A branch of AI that enables computers to understand, interpret and generate human language.

NOC Network Operations Center A centralised facility that monitors, manages and maintains an organisation's computer, telecoms, or satellite networks.

NR Network Rail The owner and infrastructure manager of most of the railway network in Great Britain, responsible for maintaining and developing rail infrastructure.

NTTNs Network Time Transfer Networks Systems are designed to synchronise time across distributed network devices to ensure accurate timestamps for data integrity and coordinated operations.

NVR Network Video Recorders A device that records footage sent digitally over a network from IP cameras, allowing for higher resolution, flexible camera placement and remote access.

O

ONVIF Open Network Video Interface Forum A global and open industry standard that enables interoperability and standardised communication between IP-based physical security devices and access control systems.

OPEX Operating Expenditure The ongoing costs an organisation incurs to run its day-to-day operations to keep the organisation functioning.

ORR Office of Rail and Road Independent regulator of railways in Great Britain, ensures compliance with safety standards using data from VSS.

P

PA/VA Public Address and Voice Alarm (systems) Integrated audio systems used in public spaces to deliver clear live or prerecorded announcements and alarms.

POV Proof of Value A process that demonstrates the measurable business valuable and tangible benefits that a security solution can deliver an organisation, helping justify adoption beyond technical feasibility.

PoP Point of Presence A physical or virtual access point where networks or devices connect to the internet or larger network infrastructure.

PpP Purchase Power Parity An economic theory comparing currency buying power across countries.

PQC Post-Quantum Cryptography The development of cryptographic algorithms designed to secure data against the potential threat of quantum computers.

PSIM Physical Security Information Management A software platform that integrates multiple disparate security applications and devices into a unified system, enabling real-time monitoring, automated workflows, and centralised control.

PTZ Pan Tilt Zoom A type of camera that can remotely rotate horizontally, move vertically, and zoom in or out to provide flexible, wide-area monitoring and detailed close-up views.

Q

QCCCS Quality, Connectivity, Capability, Coverage & Security Key performance indicators used to assess the effectiveness of video surveillance systems in enhancing rail network security.

QKD Quantum Key Distribution A secure communication method that uses principles of quantum mechanics to enable two parties to generate and share a secret cryptographic key.

R

RACI Responsible, Accountable, Consulted, Informed A project management tool that clearly defines and assigns roles and responsibilities for each task. ces processes.

RAM Reliability, Availability, and Maintainability The desired performance goals for a system to operate without failure, be operational and accessible when needed, and be quickly and easily restored after failure, aiming to optimise productivity and reduce downtime throughout its lifecycle.

RBAC Role-Based Access Controls A security model that restricts system access by assigning permissions to users based on their predefined roles within an organisation.

RDG Rail Delivery Group An organisation that brings together train companies to deliver better services; it uses VSS data to improve operational efficiency.

Glossary

ROC Regional Operations Center A centralised facility that provides expert technical support, monitoring and coordination for operational activities within a specific region.

ROSCOs Rolling Stock Operators Companies Companies that own and maintain railway vehicles leased to train operators; they use VSS data for asset protection and maintenance planning.

RSSB Rail Safety and Standards Board A UK-based organisation that works to improve the safety, efficiency, and sustainability of the railway system through research, standards development, and industry collaboration

RTAPM Regional Telecom Asset & Performance Manager A person responsible for overseeing the performance and maintenance of regional telecom and asset infrastructure, ensuring operational efficiency and compliance with safety standards

S

SASE Secure Access Service Edge A cloud-delivered framework that converges WAN capabilities with comprehensive network security functions into a single unified service.

SCADA Supervisory Control and Data Acquisition An industrial control system that enables real-time monitoring, control, and automation of processes across large geographic areas, allowing operators to manage equipment remotely.

SD-WAN Software-Defined Wide Area Network A technology that uses software to intelligently manage and optimise WAN connections, enabling secure, flexible and cost-efficient routing of traffic over multiple types of network links.

SIL Security Integration Layer A unified framework that connects and manages diverse security systems, enabling seamless data sharing, monitoring, and control across platforms

SLA Service Level Agreement A formal contract between a service provider and a customer that defines the expected level of service, performance metrics and responsibilities.

SME Subject Matter Experts An individual with deep knowledge, expertise and practical experience in a specific field or subject.

SOAR Security Orchestration, Automation and Response A cybersecurity solution that integrates and automates security tools and workflows to collect threat data, analyse incidents and manage responses.

SOCs Security Operations Centers A centralised facility within an organisation that continuously monitors, detects, investigates and responds to cybersecurity threats in real time.

SSO Single Sign On An authentication process that allows users to access multiple applications with one set of login credentials

T

TA Technical Authority Network Rail's centre of expertise, responsible for setting and maintaining technical guidance, policies, standards, processes and tools across key areas such as safety and security to ensure a safe, reliable and efficient railway system.

TfL Transport for London The local government body responsible for managing and operating the majority of the public transport network in London.

TLS Transport Layer Security A cryptographic protocol that ensures privacy, data integrity and authentication for communications over a computer network.

TOCs Train Operating Companies Companies that operate passenger trains on the railway network under franchises awarded by the government; they rely on VSS to ensure passenger safety.

U

UI User Interface The space or point of interaction where a person controls and communicates with a computer, software, or device through visual and interactive elements.

UPS Uninterruptible Power Supply An electrical device providing instantaneous backup power to connected equipment during a power outage, ensuring continuous operation and protection against data loss.

UX User Experience The overall experience a user has when interacting with a product, system, or service, encompassing usability, accessibility and emotional response.

V

VLOS Visual Line of Sight The drone pilot must maintain direct, unaided visual contact with the drone at all times during flight.

VMS Video Management Solution A system that integrates software and hardware to monitor, record, store, and manage video streams from surveillance cameras, providing a user-friendly interface for live viewing and playback

VPN Virtual Private Network A secure, encrypted connection that extends a private network across a public network, allowing users to send and receive data safely.

VSS Visual Safety & Security (Systems) Comprised of the camera, hardware connected to the camera, and monitors used to view camera footage

VTOL (drones) Vertical Take-off and Landing Hybrid drones capable of taking off, hovering and landing vertically then transitioning to efficient horizontal flight like fixed-wing aircraft.

W

WAN Wide Area Network A telecoms network that covers a large geographic area, often connecting multiple smaller networks such as LANs (local area networks).

WiFi Wireless Fidelity A wireless network technology that uses radio waves to provide devices with high-speed internet and local network connectivity without the need for physical cables.

X

XDR Extended Detection and Response A unified cybersecurity solution that integrates and correlates threat data from multiple security layers to provide comprehensive threat detection.

XML Extensible Markup Language A flexible markup language used to define, store, and transport data in a structured, human-and machine-readable format.

Z

ZT Zero Trust A cybersecurity framework that operates on the principles of 'never trust, always verify', mandating strict identity verification for every user and device attempting to access a system.

Capgemini is a global business and technology transformation partner, helping organisations to accelerate their dual transition to a digital and sustainable world, while creating tangible impact for enterprises and society. It is a responsible and diverse group of 350,000 team members in more than 50 countries. With its strong over 55-year heritage, Capgemini is trusted by its clients to unlock the value of technology to address the entire breadth of their business needs. It delivers end-to-end services and solutions leveraging strengths from Strategy and design to engineering, all fueled by its market leading capabilities in AI, generative AI, cloud and data, combined with its deep industry expertise and partner ecosystem. The Group reported 2024 global revenues of €22.1 billion.

www.capgemini.com