Digital safety

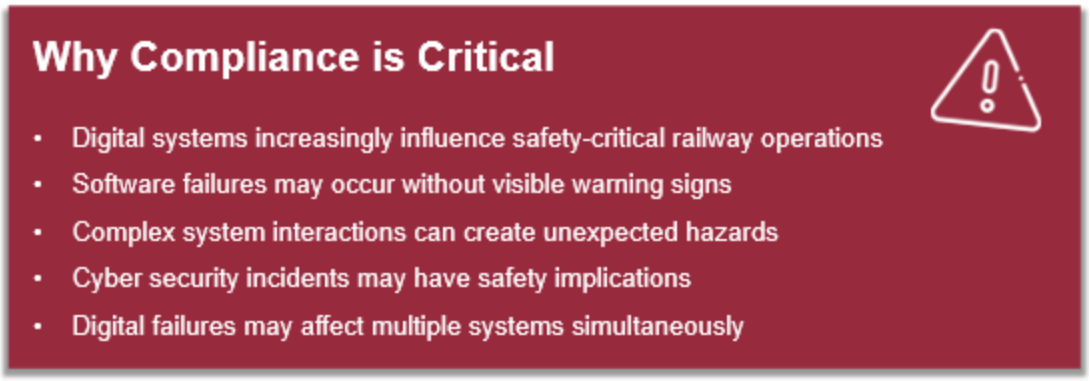
3. Compliance Expectations

Why compliance matters

Digital technologies play a critical role in the safe operation of the railway system. Software-driven systems are used to control train movements, monitor infrastructure, manage operational decision-making and support maintenance activities. These systems can directly or indirectly influence the safety of passengers, staff and the public.

As reliance on digital systems increases, the potential safety consequences of digital failures also increase. Digital failures may arise from software defects, system misconfiguration, integration failures, cyber security incidents or weaknesses in operational governance. While many digital failures result primarily in operational disruption, some may create conditions that could compromise safety if not properly controlled.

The regulatory framework governing railway safety does not distinguish between digital risks and other forms of safety risk. Dutyholders are required to manage the safety risks arising from digital systems in the same way as any other safety-critical hazard. Effective compliance therefore requires organisations to understand the role that digital systems play within their operations and to ensure that these systems are properly governed throughout their lifecycle.



The legal and regulatory basis

The management of digital safety risk is underpinned by existing health and safety legislation. These legal duties require dutyholders to manage risks arising from software based and digitally connected systems so far as is reasonably practicable. ORR expects dutyholders to manage digital safety risks as part of their Safety Management Systems (SMS) and to demonstrate that safety and security risks are controlled throughout the lifecycle of the system.

The principal legislation relevant to digital safety includes:

- Health and Safety at Work etc. Act 1974 (HSWA)
- Management of Health and Safety at Work Regulations 1999 (MHSW)
- Railways and Other Guided Transport Systems (Safety) Regulations 2006 (ROGS)
- Provision and Use of Work Equipment Regulations 1998 (PUWER)

Under sections 2, 3 and 4 of the Health and Safety at Work Act, dutyholders must take reasonably practicable measures to secure the health and safety of employees and others. This obligation applies equally to risks arising from digital systems. Moreover, section 6 of the Health and Safety at Work etc. Act 1974 places a duty on those who design, manufacture, import or supply equipment for use at work to ensure that it can be used safely.

The Act defines an “article for use at work” (s53(1)) as (a) any plant designed for use or operation (whether exclusively or not) by persons at work, and (b) any article designed for use as a component in any such plant.

Within this context, rail assets such as rollingstock, signalling systems and electrification infrastructure are all captured within this definition where they are used by workers. The software on any equipment would fall into the definition as a component in any such plant.

The Management of Health and Safety at Work Regulations place a specific duty on organisations to conduct suitable and sufficient risk assessments and to implement appropriate control measures. Regulation 3 requires dutyholders to assess risks to health and safety, while Regulation 4 establishes the general principles of prevention, often referred to as the hierarchy of control.

ROGS requires railway operators and infrastructure managers to implement an SMS capable of controlling risks arising from the operation of the transport system. These requirements apply to all risks, including those associated with digital technologies.

Regulation 18 of PUWER sets out the requirements for control systems to ensure they are safe and that they do not impede the operation of any stop controls required by Regulations 15 & 16.

Together, these legislative requirements establish the expectation that risks arising from digital systems must be assessed, managed and controlled in the same way as any other railway safety risks.

The following resources provide guidance on the identification, assessment and management of digital safety risks:

- Common Safety Method for Risk Evaluation and Assessment
- BS EN 50126:2017: Railway Applications - The Specification and Demonstration of Reliability, Availability, Maintainability and Safety (RAMS)

Cyber security and NIS regulations

The Department for Transport acts as the Competent Authority for the rail sector under the Network and Information Systems Regulations 2018 (NIS) Regulations, with responsibility for identifying Operators of Essential Services, assessing compliance and taking enforcement action where required. While ORR does not regulate cyber security directly, cyber incidents may still create safety risks. In such cases, ORR will regulate the safety implications of digital system failures under health and safety legislation.

The NIS regulations were introduced to improve the security and resilience of essential services and critical digital infrastructure across the UK. They apply to two principal groups:

- Operators of Essential Services (OES) – organisations providing services essential to societal and economic activity

- Relevant Digital Service Providers – including cloud computing services and online platforms.

Under the NIS Regulations, operators of essential services must:

- take appropriate technical and organisational measures to manage cyber security risks
- prevent and minimise the impact of incidents affecting network and information systems
- report incidents that significantly affect the continuity of essential services.

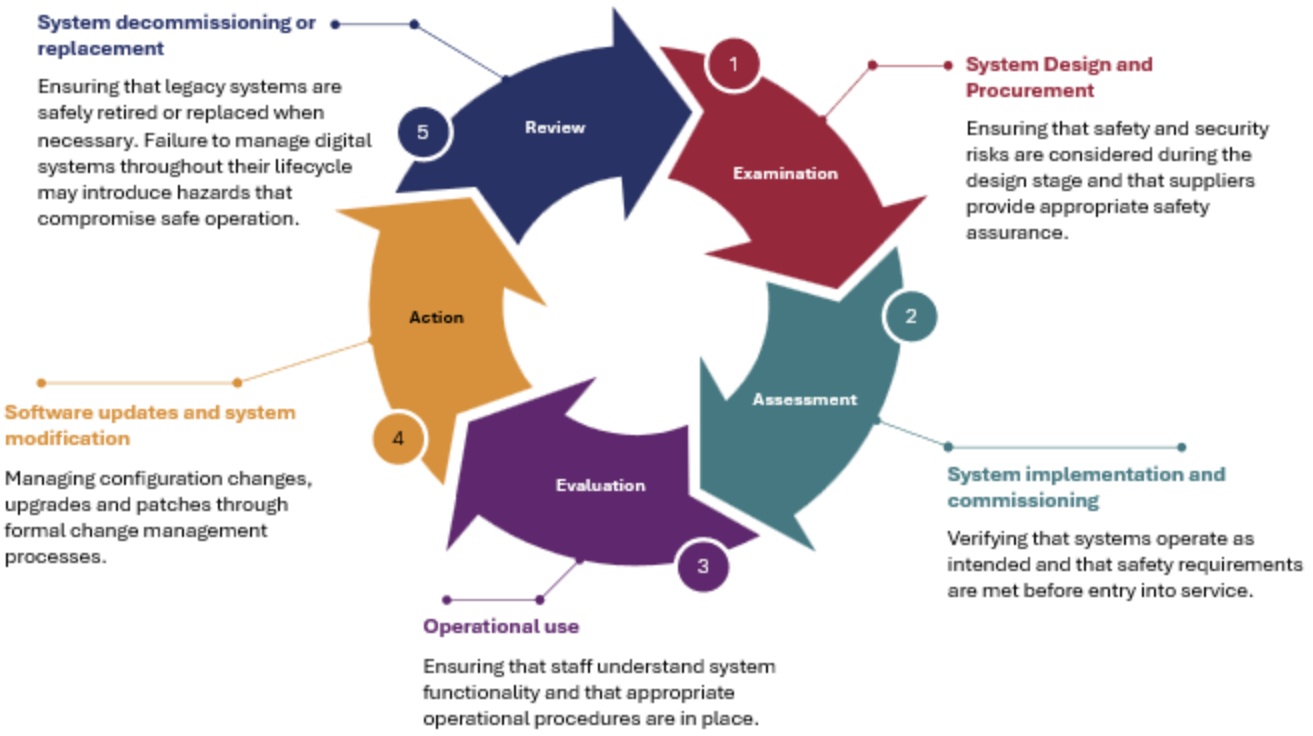
The Cyber Security and Resilience Bill (CSRB) currently going through parliament will strengthen and modernise the UK cyber resilience framework, by reforming and adding to the existing NIS regulations, including the designation of critical suppliers.

The following resources provide guidance on the identification, assessment and management of cybersecurity risks associated with Digital Systems:

- The Cyber Assessment Framework (CAF), developed by the National Cyber Security Centre (NCSC) is a tool that can be used to help organisations assess and improve their cybersecurity and resilience.
- The emerging IEC 63452 standard (Railway applications - Cybersecurity) provides cybersecurity requirements and guidance for all stages of the Digital System lifecycle.
- IET Code of Practice, Cyber Security and Safety is intended to support understanding of the issues involved in ensuring that an organisation's safety responsibilities are addressed in the presence of a threat of cyber-attack.

When compliance must be demonstrated

Compliance with digital safety obligations must be demonstrated throughout the entire lifecycle of a digital system. As another form of health and safety risk, digital safety risk must be managed through a dutyholder's SMS in the same way as other safety risk, in compliance with relevant health and safety legislation. Digital systems typically evolve through multiple stages, including design, development, procurement, installation, operation and modification. Each of these stages may introduce new safety risks if not properly managed. Dutyholders should demonstrate that digital safety risks are mitigated at each stage of the system lifecycle, as shown below.



ORR's expectations of dutyholders

ORR expects dutyholders to demonstrate that digital safety risks are properly identified, assessed and controlled within their SMS. This requires effective governance, appropriate technical competence and robust assurance processes to manage digital systems safely. Independent assurance should be employed for significant change, through use of Assessment Bodies (AsBos), independent safety assessment (ISA) and/or Independent Competent Persons (ICP) as appropriate.

In particular, dutyholders should be able to demonstrate that they:

- Maintain a clear understanding of where digital systems are used across their operations, including software that may be used in safety-critical contexts without being originally designed for that purpose;
- Treat all unexpected software behaviours as potential safety issues, identifying underlying causes and recognised risks associated with safety-critical defects are addressed;
- Demonstrate that operational mitigations or workarounds do not mask underlying safety defects or become a substitute for resolving system issues;
- Communicate and transfer safety risks between organisations, including suppliers and partners, with clear understanding of hazards, mitigations and responsibilities; and
- Define and maintain clear roles, responsibilities and ownership of digital systems and

associated risks so that accountability remains visible and effective throughout the system lifecycle.

Dutyholder checklist:

- ← Previous 2. Our view of the risk
- → Next 4. Continuous Improvement