Guidance on Rail Rolling Stock Procurement Specifications - Cyber-Security

(Version 1.0 – March 2026)

Applies to Passenger Rolling Stock Procurements in Great Britain

Issued by Land Transport National Security, Department for Transport

This Guidance is not a statement of the law. In the event of any conflict between this document and applicable legislation, the law prevails.

Contents

1. Introduction

1.1 Purpose and Scope

This Guidance sets out the key cyber-security requirements that the Department for Transport (DfT) considers should be incorporated into the specification for passenger rail rolling stock procurements, together with supporting principles that apply across the asset lifecycle. It defines the artefacts, processes, and commitments that Suppliers are expected to provide at tender and maintain throughout the lifecycle, and the preparatory actions the Contracting Authority (CA) should undertake to enable clear, evaluable, and proportionate cyber-security outcomes.

1.2 Intended Audience and Legal Status

This Guidance is **not** a statement of the law and does **not** replace or supersede any applicable legislation or regulatory obligations, including (as relevant) the Utilities Contracts Regulations 2016 and the Procurement Act 2023. If any inconsistency arises between this Guidance and applicable law, the law prevails. The Department reserves the right to amend, depart from, or rewrite any part of this Guidance where it considers it necessary or expedient. This is a dynamic document subject to controlled change; any printed copy or downloaded electronic copy is uncontrolled from the time of printing or saving.

1.3 Incorporation into Tender Documentation

The principles, expectations, and requirements set out in this Guidance shall be incorporated into the Customer's Invitation to Tender (ITT) at the pre-tender stage. The ITT shall clearly identify which elements of this Guidance are mandatory requirements, which require Supplier proposals, and which establish collaborative expectations to be developed post award throughout the lifecycle. This ensures alignment with the procurement process while providing Suppliers with clarity on cyber security outcomes, evidential expectations, and areas open to competitive differentiation.

1.4 Early Engagement with Internal Cyber Security and Engineering Expertise

The CA shall involve its internal cyber security, Operational Technology security, engineering, and operational technology teams as early as reasonably possible during development of the ITT and procurement strategy. The CA shall involve its internal cyber security, Operational Technology (OT) security, engineering, and operational technology teams as early as reasonably possible during development of the ITT and procurement strategy. Where internal capability is limited, the CA should seek external specialist expertise to ensure requirements are robust, aligned with applicable standards, and proportionate to the asset's context and risks.

1.5 Commercial Sensitivity and Transparency

The CA may receive commercially sensitive information from suppliers or other parties during pre-procurement, tender, evaluation, or negotiation stages. Such information is **not** subject to transparency requirements and may be treated as confidential by the CA. The CA shall ensure that commercially sensitive information is not disclosed to other suppliers or parties, except where disclosure is required by law. This does **not** affect the CA's obligation to provide all bidders with a consistent and transparent set of technical and cyber security requirements within the ITT.

1.6 International and Treaty State Equivalence

Where this Guidance references UK or international standards, the CA shall accept equivalent standards from treaty state suppliers in accordance with Section 56 of the Procurement Act 2023.

Suppliers claiming equivalence shall provide sufficient evidence to demonstrate functional and assurance equivalence.

1.7 Best Practice, Proportionality, and Contextual Application

This Guidance reflects best practice and is intended to support consistent, high quality cybersecurity outcomes. Its application and relevance will vary by procurement depending on system scope, risk, operational context, and lifecycle considerations. The CA should exercise proportionality and judgement when applying the Guidance, clearly documenting any reasoned deviation where appropriate would-be best practice.

Reasonable departures from this Guidance do **not** of themselves indicate that a CA has acted unlawfully; compliance with the applicable law remains the overriding obligation.

1.8 Bid Evaluability and Assessment Requirements

The CA is responsible for developing an evaluation framework that enables clear, consistent, and defensible assessment of Supplier cyber security bids. The framework shall ensure that all bids can be compared on an equal basis, with traceability from each requirement in the ITT to the corresponding evidence submitted by the Supplier.

This Guidance does **not** prescribe specific templates or formats. The CA shall determine the structure, tools, and documentation it considers appropriate for its procurement, ensuring that the requirements set out in the ITT are evaluable, proportionate, and aligned to the specifics of each procurement strategy.

2. Contracting Authority Pre Tender Obligations

Purpose
This section defines the baseline cyber security principles, standards, and pre-tender obligations that the CA must establish before issuing the ITT. It sets out the foundational decisions, specifications, and responsibilities required to ensure suppliers can prepare compliant, proportionate, and fully informed cyber security bids.

2.1 Baseline Cyber Security Standards and Design Principles

2.1.1 Applicable standards
Rolling stock and associated supporting tools shall be designed to be cyber secure in compliance with standards recognised as applicable to Railway Operational Technology (for example IEC 62443 series, **IEC 63452** [recommended], and PD CLC/TS 50701).

2.1.2 Lifecycle adoption of updated standards
Provision shall be made to review and, where reasonably practicable and mutually agreed, incorporate updated or additional standards during the lifecycle to maintain an appropriate level of cyber security. Such adoption will primarily apply to systems or assets introduced after initial delivery and shall not impose retroactive obligations on assets delivered under standards agreed at tender stage, unless mutually agreed and practicable ahead of acceptance of the first unit.

2.1.3 Lifecycle coverage
Cyber security requirements apply throughout the operational lifecycle, including mid-life upgrades, retrofits, and replacements. All parties shall ensure that any new or modified components introduced during the lifecycle are designed, integrated, and assured to maintain or improve the overall cyber security posture in accordance with applicable standards agreed at the time of the upgrade and the best practices in this Guidance.

ITT — What to include for 2.1:

• Identify the baseline standards to be applied and the governance for adopting updates.
• The point at which updated standards become applicable (e.g., new systems only).
• Confirmation of lifecycle coverage (upgrades, retrofits, replacements).

2.2 Foundational Cyber Security Decisions Prior to Tender for the Contracting Authority

2.2.1 Initial risk assessment

The CA shall perform an initial risk assessment of the operational context and associated risks at the point of tender. This assessment shall be shared with bidders to inform proposals and enable suppliers to propose appropriate security levels for the asset and, where relevant, for key systems. All bids must specify the proposed security level for the asset in accordance with IEC 62443 or IEC 63452.

2.2.2 Target security level (optional)

At the discretion of the CA, the risk assessment may be used to define a desired target security level for the asset using the processes in IEC 62443 or IEC 63452, which shall be communicated at tender. The Supplier shall then propose how these security levels will be achieved at the subsystem and, where necessary, component level to ensure overall asset security and integrity. The CA may also outline specific security levels for certain subsystems or components where deemed necessary.

ITT — What to include for 2.2:

• CA risk assessment summary (enough to support bidders' SL proposals).
• Any CA mandated target security levels and rationale.

2.3 Shared Responsibilities for Secure Operations and Collaboration

2.3.1 Customer obligations and supplier dependencies

The CA is responsible for setting the required cyber security standards and obligations within the ITT and contract documentation. The Supplier shall also identify and maintain a register of dependencies on the Customer, maintainer, ROSCO, and operator required to uphold the efficacy of the agreed cyber security controls and measures.

These dependencies shall be:

a) Explicitly stated in contractual and technical documentation;
b) Explained with reference to relevant security objectives/standards;
c) Reviewed and updated during lifecycle reviews to reflect changes in configuration, context, or standards.

2.3.2 Secure maintenance regime and TSA

All parties responsible for maintaining rolling stock and associated systems shall ensure their supporting systems, processes, and practices maintain a secure maintenance regime, including access controls, secure data handling, and protection of diagnostic/configuration tools. The Supplier shall collaborate with the maintainer to produce a Technical Service Agreement (TSA) to be shared with the Customer, outlining controls to maintain a secure regime and specifying any Customer responsibilities.

2.3.3 Vulnerability realism and collaboration

The CA acknowledges that achieving vulnerability free rolling stock is unrealistic. All parties (Supplier, maintainer, ROSCO, Operator) commit to work collaboratively and in good faith throughout the lifecycle to identify, assess, eliminate or mitigate, and manage vulnerabilities and associated risks. The Supplier shall work with Operators and owners from the earliest stages to ensure continuous validation and proactive risk management throughout the lifecycle.

ITT — What to include for 2.
• Request a "Supplier Dependencies Register".
• TSA requirement and minimum security controls to be covered.
• Principles for collaborative vulnerability management (incl. risk acceptance).

2.4 Assurance Approach, Independence & Competence Requirements for Tender Submissions

2.4.1 Assurance expectations and relationship to safety assurance

The CA shall require a cyber security assurance process that applies throughout the development and operational lifecycle (including design, development, integration, and mid-life updates). This cyber security assurance is separate from and additional to safety and interoperability assurance performed by the NoBo/AsBo.

The CA may either:
a) Specify a desired assurance regime to be followed by the Supplier; or
b) Require bidders to propose their own assurance regime, including justification and costings.

2.4.2 Acceptable assurance methods

Any assurance regime, whether CA specified or Supplier proposed, shall use one or a combination of the following accepted methods:

a) Independent third party assessment; or
b) Supplier led internal validation and verification processes.

2.4.3 Bidder assurance proposal requirements

Where bidders are required to propose their own assurance regime, the Supplier shall outline their approach at bid stage, including costings, rationale, and applicable methods.

All assurance regimes (CA specified or Supplier proposed) shall ensure:

a) Continuous assurance throughout the lifecycle, not limited to initial acceptance;
b) Clear documentation and evidence provided to the Customer, including a signed and named statement from the responsible individual or organisation specifying:

- the scope of assurance;
- what has been assessed;
- the results and any recommendations provided to the Supplier.

2.4.4 Cyber Security Acceptance Gates

To ensure secure-by-design principles are embedded throughout the lifecycle, the Supplier shall commit at bid stage to a Cyber Security Acceptance Gate regime. Bidders shall outline their proposed Acceptance Gates, including indicative timing, alignment to their development plan, and any assumptions or dependencies.

During contract finalisation, the CA and Supplier shall define and confirm the final set of Cyber Security Acceptance Gates. These gates:

a) Shall align with the rolling stock project lifecycle (e.g., Design Freeze, First Article, Type Test, Pre APIS, APIS, Entry into Service).
b) Shall specify the minimum cyber security artefacts, tests, evidence, and required remediations for progression, as detailed in Section 3.

c) Shall integrate with safety and technical assurance processes without duplicating effort.
d) Shall be fully agreed prior to the commencement of design activities.

The Supplier shall not progress beyond an Acceptance Gate until the CA has confirmed acceptance of the required cyber security artefacts or has agreed a deviation or mitigation.

2.4.5 Independence for supplier led V&V
Where a supplier led internal V&V process is used, the Supplier shall demonstrate that this process is independent and organisationally separate from the teams responsible for design and implementation.

2.4.6 Competence for third-party assessors
Where an independent third-party expert is appointed, they must demonstrate **proven experience** applying cyber security standards in rail/OT environments, expertise in attack methods, risk assessment, and security practices, hold relevant certifications (e.g., CISSP, CISM, GIAC), and have practical experience with complex OT systems and railway safety/software standards. Certifications alone are insufficient; evidence of capability and experience is required to ensure assurance is fit for purpose.

ITT — What to include for 2.4:

- *Assurance plan (method, scope by lifecycle stage, independence model) or request for bidders to outline, including acceptance gates*
- *Named responsible individual/organisation and example statement template.*
- *CVs/credentials and evidence of relevant OT/rail experience (for third party) and/. Or organisational separation evidence (for internal V&V).*

2.5 Mandatory Cyber Security Penetration Testing Requirements

2.5.1 Whitebox penetration test prior to operational approval
The CA will require suppliers to commission a white-box penetration test of the rolling stock and supporting wayside tools/systems as the final cyber security validation before finalising operational approval. The test shall be conducted by NCSC CHECK accredited testers or by a penetration tester selected and approved by the Customer.

2.5.2 Secure handling of results
Results shall be shared under agreed protocols suggested by the Supplier to ensure safe and secure handling. All parties must ensure that test results are transmitted, stored, and accessed only within secure environments, with appropriate technical and procedural controls.

2.5.3 Relationship to standards compliance
Penetration testing is a necessary and complementary activity that supports validation of compliance with cyber security standards (see 2.1). It is not sufficient on its own; compliance must be demonstrated through the broader assurance regime in 2.4 and the artefacts in Section 3.

2.5.4 Scope agreement and representativeness
The test scope shall be agreed collaboratively by the Operator, ROSCO, Supplier, and penetration tester. The unit and associated systems tested shall be in a configuration representative of the intended passenger service configuration and functionality.

2.5.5 Vulnerability assessment and remediation
Vulnerabilities identified shall be assessed collaboratively, focusing on exploitability and risk. Casual (easily exploitable) vulnerabilities shall be prioritised and remediated. The Supplier shall demonstrate how other identified vulnerabilities align with the procured specification through Security Level risk assessments (see 3.3.4). Where remediation requires changes beyond original scope, variation orders shall be negotiated in good faith.

ITT — What to include for 2.5:
• Proposed pen test partner(s) and accreditation(s) or request for suppliers to arrange included in bid.
• Draft evidence handling protocol, and secure environment controls.
• Remediation prioritisation approach and linkage to SL risk assessments.

2.6 Additional Pre Tender Specifications Required

Before issuing the ITT, the CA shall review all Supplier expectations set out in Section 3 and ensure that the information required for a compliant bid is provided in advance. The CA shall consider the implications of each clause and supply sufficient clarity to enable Suppliers to develop accurate, complete, and costed proposals.

Particular consideration shall be given to areas where the CA is required to specify parameters or make pre-tender decisions, including:

- **3.2 Scope of Supply** – definition of in scope systems, components, testing assets, and any Customer provided infrastructure.
- **3.3 Data Protection** – identification of personal data processed, relevant data flows, and Customer data protection requirements.
- **3.6 Monitoring Provision** – required monitoring level, systems to be monitored, IDS expectations, and integration with Customer SOC or equivalent.
- **3.7 Service Recovery** – response and recovery time objectives, escalation expectations, and coordination requirements.
- **3.10 Training** – number of staff requiring training, locations, and specific operational/maintenance competencies required.
- **3.12 Physical Security Considerations** – any mandated physical protection requirements or minimum-security levels for critical subsystems or equipment.

These requirements shall be clearly set out in the ITT to ensure Suppliers can prepare compliant, consistent, and evaluable bids.

3. Supplier Bid Submission Cyber Security Expectations

Purpose
This section specifies the artefacts, commitments, and evidence that bidders are expected to provide or commit to providing to demonstrate adequate cyber security for rolling stock and associated systems, and to enable operators to maintain secure operations throughout the assets lifecycle.

3.1 System Cyber Security Objectives

3.1.1 Objective

The purpose of the cyber security requirements is to:

- Eliminate identified cyber risks where reasonably practicable.
- Where elimination is not possible, minimise exposure to the cyber threat environment, including unauthorised access, theft, malfunction, failure, and incorrect or corrupted data inputs that could cause undesirable outputs without full onboard system malfunction.

3.1.2 For the purposes of this document this includes:

a) Identifying all system components, vulnerabilities, threats, and risks.
b) Specifying controls to mitigate the risks.
c) Monitoring the system to ensure controls remain effective.
d) Detecting unauthorised activity or breaches.
e) Responding to contain the activity.
f) Recovering and resuming normal service.

3.1.3 Customer support
Provide support to the Customer to contain and recover from cyber security incidents, including actions addressing root cause.

3.1.4 Regulatory cooperation (NIS Regulations 2018)
Support the Customer's compliance by providing cooperation and evidence required for accurate fulfilment of regulatory obligations.

3.1.5 Supplier-wide risk management
Ensure all Supplier internal operations and all systems and assets delivered to the Customer are managed to minimise cyber security risk throughout their lifecycle. Therefore:

- **a) Information security certification**
  Suppliers of key IT related services must hold certification to a recognised Information Security standard (e.g., **BS EN ISO/IEC 27001** or **Cyber Essentials Plus**) with scope covering the services provided. Where certification is not held, equivalent evidence of compliance must be provided.

- **b) Cyber Security Management Plan (CSMP)**
  Systems and services delivered to the Customer must be governed by a CSMP that identifies, mitigates, and manages cyber risks throughout the lifecycle to a level acceptable to the Customer. Where lifecycle support is not included, the CSMP — together with any source code escrow arrangements and the software requirements set out in Section 3.11 — must provide sufficient detail to enable the Customer to maintain cyber security to an acceptable level post-delivery.

Bid submission — What to include for 3.1:
• Statement of objectives and approach to risk elimination/minimisation.
• Certificates (e.g., ISO/IEC 27001 scope & statement of applicability; Cyber Essentials Plus), or equivalent evidence of key IT-related services including how suppliers supply chain risks are managed
• High-level description of the CSMP scope and governance model.

3.2 Scope of Cyber Security Supply

3.2.1 Applicability

- These requirements assume compliance with **3.1.5(a)** (Supplier internal practices) and focus on what is necessary for **3.1.5(b)** (CSMP governed delivery).

3.2.2 Customer requirement

- The Customer requires the design and supply of cyber security controls for its rail vehicles.

3.2.3 Scope of supply

- Includes all hardware, software, and associated equipment necessary to support the Customer's cyber security activities.

- Includes sample equipment and software for security testing, unless explicitly opted out by the Customer.
- All such arrangements must be confirmed and agreed by all parties prior to acceptance of the first unit into service.

3.2.4 Coverage

- Cyber security requirements apply to all components that use software (including firmware) in their operation, whether or not they are connected to onboard networks.

ITT – What to include for 3.2:

- *Declare whether sample equipment and software for security testing are required in the bid*

Bid submission — What to include for 3.2:
• Bill of supply identifying in-scope systems, interfaces, and sample/testing assets.
• Confirmation of coverage for all software using components.
• Any proposed exclusions with justification.

3.3 Core System Artefacts & Governance

3.3.1 Cyber Security Management Plan (CSMP)
Provide and maintain a CSMP for each digital system/service aligned with **IEC 63452** for rolling stock or an equivalent recognised standard (e.g., **IEC 62443**, **ISO/IEC 27001**) for other systems. The CSMP must define governance, roles, responsibilities, and a lifecycle cyber security approach including threat monitoring, vulnerability management, and timely updates throughout operational life.

3.3.2 Software & Hardware Catalogue (SBOM/HBOM)
Provide to the maintainer and Customer a catalogue that includes:

a) manufacturer;

b) name;

c) version;

d) for hardware, the modification state (mod state) covering updates/changes from original build (firmware updates, component replacements, etc.);

e) known vulnerabilities for each component.

The SBOM/HBOM is a highly sensitive asset and shall be handled under a jointly agreed secure management process to be outlined by the Supplier. This process shall govern distribution, storage, access control, and audit logging to ensure confidentiality, integrity, and protection against unauthorised disclosure.

Where the Supplier retains responsibility for maintenance, SBOM/HBOM information shall be made available at a level sufficient to support Customer assurance, incident response, and regulatory obligations. Where maintenance responsibilities transfer to the Customer or maintainer, full operational access to the SBOM/HBOM shall be provided.

3.3.3 SBOM/HBOM Operational Requirements

The Supplier shall operationalise SBOM and HBOM management throughout the lifecycle, ensuring they remain accurate, current, and suitable for ongoing cyber security assurance. Accordingly:

a) **Update Cadence**
SBOM/HBOMs shall be updated:
• At each software release.
• Following any firmware or hardware modification.
• At regular intervals proposed by the Supplier and subject to agreement with the CA for the operational lifecycle.

b) **Format Requirements**
SBOMs shall be provided in a recognised machine readable industry format such as CycloneDX or SPDX, with HBOMs provided in an equivalent structured format.

c) **Vulnerability Attestation**
The Supplier shall provide, at regular intervals proposed by the Supplier and subject to agreement with the CA, an SBOM/HBOM delta identifying:
• newly disclosed vulnerabilities,
• risk assessments (aligned to IEC 62443 / 63452),
• proposed mitigations or compensating controls.

d) **Tamper Evident Delivery**
All SBOM/HBOM artefacts shall be delivered using tamper evident mechanisms (e.g., cryptographic hash, digital signature, or secure file transfer with integrity verification).

e) **Access Auditing**
The Supplier shall maintain audit logs for all access to SBOM/HBOM repositories and provide audit reports to the Customer upon request.

f) **Secure Storage & Handling**
SBOM/HBOMs shall be stored, transmitted, and accessed only through secure, access controlled environments agreed with the CA.

3.3.3 Technical documentation
Develop, maintain, and provide accurate, current documentation throughout the contract and operational lifecycle, including:

a) **Data flows** between all system components;
b) **Protocols and ports** used;
c) **Encryption** protocols/modes/parameters for data at rest and in transit.

3.3.4 Risk assessments & security levels
Undertake and maintain cyber security risk assessments in accordance with IEC/ISA 62443 and IEC 63452. Assessments shall cover each subsystem, zone, and major component to define the target security levels and shall be shared with the Customer.

Where an achieved security level falls below the specified overall level for the train asset, the Supplier shall provide a justification, including an analysis of available market alternatives.

The Supplier shall continuously evaluate and document the capability security level as the design develops and shall provide updates throughout the asset lifecycle as part of ongoing assurance.

3.3.5 Data protection
Where personal data is processed, conduct a Data Protection Impact Assessment (DPIA) aligned with the Customer's data protection requirements and implement all actions to achieve an acceptable residual risk as determined by the Customer.

ITT — What to include for 3.3:

- Outline Data protection requirements (if any) for this procurement for suppliers to adhere to

Bid submission — What to include for 3.3:
• CSMP (or outline with contents list and standard alignment if final will follow at award).
• Initial SBOM/HBOM (or process and frequency if full detail depends on final design), and SBOM handling controls.
• Draft technical documentation pack (data flows, ports/protocols, crypto).
• Risk assessment approach, security level rationale, and initial results if available.
• DPIA approach (and DPIA if applicable).

3.4 Security Controls & Access Management

3.4.1 Control set identification & maintenance
Identify the security controls applied to achieve the defined security level(s). Define intervals/requirements for maintaining these controls and agree them with the maintainer, who is responsible for lifecycle implementation.

3.4.2 Access control & password reconfiguration
Each subsystem shall include access controls enabling the Customer to manage user access at the highest privilege level. **All default passwords/credentials** must be **easily reconfigurable** by the Customer **before APIS** (Authorisation to Place Into Service) or equivalent handover. Passwords shall comply with recognised standards (e.g., **IEC/ISA 62443**, **IEC 63452**) and best practice; provide evidence before acceptance.

3.4.3 Limitations & roadmap
Where password management or security control changes are not supported, disclose limitations at bid and propose options or a roadmap for enabling capabilities, subject to Customer prioritisation and agreement.

3.4.4 Privileged access (pre-handover)
The Supplier may nominate individuals requiring privileged access for commissioning/support prior to handover. Nominations must be risk justified and agreed with the Customer.

3.4.5 Vetting
All individuals granted privileged access must be vetted per standards agreed between Supplier and Customer. Vetting/authorisation criteria shall be jointly defined and aligned with the system's security level and governance.

3.4.6 Privileged access (post handover)
Any ongoing privileged access after handover shall be defined in the TSA and agreed between Customer, maintainer, and Supplier in accordance with IEC 63452 processes.

3.4.7 Remote access & MFA
Where systems include remote access or managed services, implement multi-factor authentication (MFA) as a baseline control. Where MFA is not feasible, provide justification for Customer approval.

Bid submission — What to include for 3.4:
• *Controls catalogue mapped to security level(s) and standards.*
• *Evidence of password policy, changeability, and secure credential handling.*
• *Privileged access model, vetting standard, and pre/post handover arrangements.*
• *Remote access architecture and MFA approach (or justified exceptions).*

3.5 Security Testing, Validation & Revalidation Plan

3.5.1 Test scope & purpose
Conduct security tests to determine achieved security level for each subsystem, zone, and major component at key milestones (including prior to final delivery) and at the agreed cybersecurity gates

(see Section 2.4.4) throughout operational life, especially after major updates, configuration changes, or discovery of new vulnerabilities.

3.5.2 Triggers for re-validation

Major updates and changes in scope include, but are not limited to, changes affecting system architecture, authentication mechanisms, data flows, network interfaces, firmware, software components, or any change that could alter the system's security posture or introduce new vulnerabilities.

3.5.3 Coordination

Coordinate with the maintainer to establish frequency, scheduling, and scope of tests. Ensure the maintainer understands obligations for regular testing and revalidation under the **TSA**.

Bid submission — What to include for 3.5:

• Security test strategy and plan (methods, environments, tools, independence of testers).
• Test evidence expectations (e.g., results, findings, mitigations, re-test).
• Re-validation triggers and cadence.
• Proposed responsibilities split with maintainer and third parties.

3.6 Monitoring & Detection of Unauthorised Activity

3.6.1 General Requirement for Monitoring in Bids

All bids shall include provisions for system monitoring. As part of the tender, the Customer will specify the expected level of monitoring, scope (systems and subsystems), and whether the requirement applies to the full fleet or a representative subset. Intrusion Detection Systems (IDS) are recommended as a baseline capability where technically feasible.

3.6.2 Default Monitoring Provision (Where Not Specified)

If the Customer does not specify monitoring requirements, the Supplier shall propose appropriate monitoring arrangements as part of the bid. This shall include all parties actively managing the asset or service (including managed service providers and maintainers). The Supplier shall confirm:

- subsystems monitored and responsible parties;
- monitoring frequency;
- methods used to detect unauthorised activity;
- reporting and escalation routes to competent personnel.

These obligations shall be incorporated into the TSA (or equivalent) to ensure continuity throughout the lifecycle.

3.6.3 Incident Notification

All Suppliers and maintainers shall notify the Customer of any cyber security incident affecting their own systems or infrastructure that may impact the supplied system. An initial assessment of potential impact shall be provided as soon as reasonably practicable.

3.6.4 Operational Monitoring Requirements

To demonstrate how the monitoring obligations in 3.6.1–3.6.3 will be achieved, the Supplier shall provide detailed operational monitoring arrangements as part of the bid and maintain these arrangements throughout the lifecycle. These arrangements shall include, but not be limited to:

a) Monitoring Data Sources

Identification of all relevant monitoring data sources, including:

- system logs, security logs, network traffic records, sensor telemetry, diagnostic outputs, configuration change logs;
- data retention periods (minimum 12–24 months recommended);
- time synchronisation mechanisms (e.g., NTP/GPS), including drift tolerances for timestamp integrity.

b) Monitoring Architecture

A description of the monitoring architecture sufficient for assurance of integrity, confidentiality, and availability, including:

- onboard log collection and secure storage;
- transfer of monitoring data and alerts from onboard → wayside → Customer systems;
- secure transmission methods (e.g., TLS 1.2+, certificate management, encryption approaches);
- use of IDS or behaviour based anomaly detection where feasible.

c) Alerting & Escalation Requirements

Definition of:

- severity levels and detection thresholds;
- recipients for alerts (e.g., Supplier support team, maintainer, Customer SOC);
- response SLAs for Severity 1–3 events aligned with Customer incident response expectations;
- integration with Customer and maintainer escalation processes.

d) Access and Audit Controls

Monitoring arrangements shall include appropriate controls to prevent tampering or unauthorised access, including:

- role-based access to monitoring data;
- tamper protection or integrity validation for log stores;
- audit logging of access and configuration changes;
- availability of audit reports to the Customer on request.

ITT – What to include for 3.6:

- *Specify required level of monitoring, particularly if full IDS of each asset is required.*
- *the Customer's incident response expectations;*
- *draft Customer and maintainer escalation processes.*

Bid submission — What to include for 3.6:

- *A monitoring architecture description including onboard, wayside, connectivity and data transfer arrangements.*

- *A statement of monitoring coverage, data sources, retention periods, and synchronisation methods.*
- *IDS implementation or alternative monitoring plan with justification.*
- *Alerting and escalation pathways, including severity thresholds and SLAs.*
- *Tamper protection and audit mechanisms.*
- *Incident notification and communication processes.*

3.7 Service Recovery

3.7.1 Containment
Define how detected events can be contained within the system/service, including isolation or deactivation of affected components.

3.7.2 Supplier support
Propose how the Supplier will support incident response and recovery related to the system/services provided. Include indicative response and recovery times, prioritisation, and escalation processes, emphasising coordination between maintainers, third parties, and stakeholders. Outline resources, tools, and processes to deliver these commitments.

3.7.3 Customer definition
The Customer will define required support levels (minimum response/recovery time objectives, escalation, coordination). These shall form the basis for contractual agreements under the **TSA** or equivalent, ensuring clarity on roles and responsibilities throughout the lifecycle.

ITT – What to include for 3.7:

- *Definition of required support levels in service recovery*

Bid submission — What to include for 3.7:
• Containment playbooks/runbooks and isolation mechanisms.
• Proposed incident response & recovery SLAs (RTO/RPO if relevant).
• Team structure, on call model, and authority matrix.
• Dependencies on Customer/maintainer/third parties.

3.8 Safety

3.8.1 Safety compliance

Cyber security–related hazards shall be managed in the same manner as any other safety hazard, in compliance with applicable legislation and standards, including the Railways and Other Guided Transport Systems (Safety) Regulations 2006 (ROGS), the Technical Specifications for Interoperability (TSIs), the Network and Information Systems (NIS) Regulations, and the Common Safety Method for Risk Evaluation and Assessment (CSM-REA).

The Supplier must identify any cyber risks that could represent a safety hazard and implement control measures to the level required by law.

3.8.2 Process integration

Cyber hazard identification shall be integrated into both the Customer's and Supplier's safety processes and include consultation with all relevant stakeholders. Cyber security considerations shall be reflected in hazard logs, safety assurance arguments, and associated mitigations.

3.8.3 Safety case impact

The Customer will determine whether identified cyber related hazards impact its regulatory safety case. Where cyber security considerations affect the safety case, mitigation strategies shall be agreed between the Customer and Supplier and documented.

3.8.4 Cyber–Safety Traceability Requirements

The Supplier shall ensure explicit traceability between cyber security controls and safety related hazards throughout the lifecycle. This traceability shall include:

a) Mapping CSMREA Hazard IDs to relevant cyber security risks and the controls applied to mitigate them.

b) Linking each cyber security control to its corresponding:
• applicable Security Level (SL) requirement;
• test evidence, including verification, validation, and penetration testing results;
• related CSC claims, arguments, and evidence.

c) Ensuring that cyber derived safety hazards are reflected in:
• safety hazard logs,
• the Safety Case,
• the Cyber Security Case,
• and associated mitigations.

d) Maintaining traceability across design updates, configuration changes, incident learnings, and midlife upgrades.

Traceability matrices shall be submitted at bid and updated throughout the asset lifecycle.

3.8.5 Cyber Security–Safety Conflict Resolution and Change Control

Where conflicts arise between cyber security updates (e.g., security patches, configuration changes, mitigations) and safety certification requirements, the Supplier shall follow a defined conflict resolution and change control process. This process shall include:

a) Convening a **Change Control Board (CCB)** chaired by the Customer, with representation from:
• Supplier design authority,
• Maintainer,
• ROSCO,
• Safety assessor (AsBo/ISA),
• Operator (where applicable).

b) Assessing the proposed change in terms of:
• cyber security risk,
• safety impact,
• operational consequence,
• regulatory compliance.

c) Determining whether the change can proceed, requires mitigation, or must be deferred.

d) Documenting all decisions and ensuring alignment with the Safety Case and Cyber Security Case.

No security update affecting a safety related function shall be deployed without CCB approval.

Bid submission — What to include for 3.8

- *A description of the safety–cyber integration approach, showing how cyber considerations enter safety processes and hazard logs.*
- *A traceability matrix mapping:*
  • CSM-REA Hazard IDs → Cyber risks → Cyber controls → SL requirements → Test evidence → CSC references.
- *Evidence demonstrating how cyber controls mitigate safety related hazards.*
- *Proposed engagement cadence with safety assessors, verifiers (AsBo/ISA), and Customer stakeholders.*
- *Commitment to collaborating with Change Control Boards or equivalent*

3.9 Additional Documentation (Cyber Security Case)

3.9.1 Documentation set
In addition to the Asset Portfolio & Catalogue and the CSMP, provide the following documentation maintained throughout the asset lifecycle.

3.9.2 Cyber Security Case (CSC)
Develop and maintain a single unified CSC for the rail asset, covering safety and non-safety assurance arguments. Safety related evidence can be referenced from the Hazard Record, Safety Case, and CSM Safety Assessment Report. Initiate the CSC following contract award and no later than commencement of design, maintain throughout the lifecycle, and review/update at least annually.

3.9.3 CSC standard alignment & content
Develop the CSC in accordance with IEC 63452 and/or PD CLC/TS 50701, or equivalent recognised standards. The CSC shall include, at minimum:
a) identification/assessment of threats & vulnerabilities;
b) risk management & mitigation strategies;
c) security controls & assurance measures;
d) evidence of compliance with applicable standards & requirements;
e) integration of relevant existing CSCs for subsystems/components, with clear references/traceability.

3.9.4 Multi-party involvement
The supplier must develop and maintain the CSC with the involvement of all relevant parties: manufacturer, ROSCO, operator, maintainer - to ensure shared understanding and accountability.

3.9.5 Responsibility
Responsibility for maintaining the CSC rests with the design authority (Supplier) during design, build, commissioning, and throughout the lifecycle, unless expressly transferred under separate contractual terms. Any transfer must be documented in a dedicated agreement explicitly assigning CSC maintenance obligations. In absence of such agreement, the Supplier retains full responsibility.

3.9.6 Handover documentation
Provide all handover documentation required by **IEC 63452**, including configuration, maintenance, and operational guidance not already covered in the CSC.

3.9.7 Avoiding duplication
Where information is already provided in the Asset Portfolio & Catalogue, CSMPs, or other submissions, it need not be duplicated in the CSC or vice versa if clearly referenced and sufficiently covered.

Bid submission — What to include for 3.9:
• CSC structure (argument patterns/claims), standards alignment, and production plan.

• Responsibility matrix and governance for updates & multiparty inputs.
• Handover documentation plan and cross-references.

3.10 Training

3.10.1 Purpose
Training obligations support the Customer's internal capability development and **do not** replace any maintenance/performance responsibilities under the TSA or other agreements.

3.10.2 TraintheTrainer
Provide Train-the-Trainer for an agreed number of operational and maintenance staff (proportionate to Customer staffing) to ensure sufficient capability to maintain/operate the system. Training shall take place before system delivery at a Customer chosen location.

3.10.3 Content & timing
Cover system fundamentals, architecture, and intended modes of operation relevant to the delivered system. Deliver prior to system delivery at a Customer chosen location.

3.10.4 Tools & simulations
Provide training using test tools and simulations for an agreed number of technical staff, enabling detection of cyber breach indicators, recognition of signs, and effective response per agreed procedures.

3.10.5 Training materials
Provide all training artefacts (presentations, notes, videos, training plan) to the Customer.

ITT – What to include for 3.10:

- *Number of personnel to be trained, by role.*
- *Required training locations and any constraints.*
- *Required delivery timeframe.*
- *Mandatory content or competencies to be covered.*
- *Any Customer-provided tools, simulators, or environments to be used.*

Bid submission — What to include for 3.10:
• Training syllabus, audience, duration, and delivery method.
• Lab/demo tooling to be provided and any licensing.
• Materials list and delivery schedule.

3.11 Software Development & Patching

3.11.1 Development standards
Develop and update software throughout the lifecycle in compliance with BS EN 50126, BS EN 50129, and BS EN 50716. The superseded standards BS EN 50128 and BS EN 50657 may be applied where subsystems have prior assurance and still valid certifications.

3.11.2 NCSC Software Security Code of Practice
Subscribe to the NCSC Software Security Code of Practice and complete the self assessment for each subsystem/product comprising the rolling stock and associated systems. Identify:

- responsibility for patch management of each subsystem;
- indicative lifecycle costings for security updates;
- any components not supported for the full expected lifecycle of the rail asset (minimum 40 years unless otherwise specified).

3.11.3 Supply chain arrangements

Establish documented agreements across the supply chain and with maintainers to ensure timely patching and vulnerability management throughout the lifecycle. Capture these in the TSA or equivalent and review periodically to address obsolescence and emerging threats.

3.11.4 Supply Chain Cyber Security Ownership

The Supplier shall identify, document, and maintain clear ownership of all cyber security responsibilities across its supply chain. This shall include:

a) Named owners for patch management, vulnerability tracking, obsolescence management, and incident coordination for each subsystem and software/hardware component.
b) Defined escalation paths and response SLAs across all suppliers and sub suppliers.
c) Evidence that supply chain partners have appropriate cyber security capabilities and can meet lifecycle obligations, including timely patching and vulnerability remediation.
d) A clear and readable mapping of cyber security responsibilities across the supply chain, such as a RACI matrix or an equivalent responsibility mapping tool, aligned with the roles of the Customer, Supplier, maintainer, ROSCO, and relevant third parties.

The Supplier shall submit this information as part of the bid and maintain it throughout the lifecycle.

3.11.5 Obsolescence & escrow

The Supplier shall detail the software obsolescence management approach, including: source code escrow, minimum end of support notice periods, and obligations for security patching beyond OEM lifecycle. Provide a minimum of five (5) years' advance notice prior to end of support for any software component.

Bid submission — What to include for 3.11:

- *Development standard alignment and assurance approach (including SIL where applicable).*
- *Completed or draft NCSC SSCoP self assessments.*
- *A detailed description of patch management and vulnerability processes, including SLAs.*
- *A supply chain cyber security RACI matrix or equivalent evidence of partner competence.*
- *Supply chain escalation paths and incident coordination arrangements.*
- *Obsolescence and escrow plan, including end of support commitments and the minimum advance notice to end of support commitment*

3.12 Physical Security Considerations

3.12.1 Measures & longevity

The supplier must identify physical security measures to protect onboard equipment from unauthorised access, reflecting system criticality. Include appropriate access controls for maintainers, drivers, and driver managers, and provide an estimate of security control longevity and maintenance regime.

3.12.2 Customer mandates & ETCS

Where specific/advanced solutions are required, the Customer shall mandate these at tender. For **ETCS** equipment, align measures with **RIS-0340** principles.

ITT – What to include for 3.12:

- *Any mandated access-control expectations for maintainers, drivers, or driver managers.*
- *Any advanced or bespoke physical protections the Customer expects*
- *Any ETCS-specific physical security expectations where applicable.*

Bid submission - What to include for 3.12:
• Physical protection design (tamper resistance, seals, enclosures, access control).
• Key/credential handling for physical access; audit & logging methods.
• ETCS specific measures (if applicable) and standard alignment.

3.13 Deviations, Assumptions & Dependencies

3.13.1 Deviations
List any deviations from these requirements with clear justification, risk assessment, and proposed compensating controls/mitigations.

3.13.2 Assumptions
State all assumptions underpinning the bid (technical, operational, commercial).

3.13.3 Dependencies
Identify dependencies on Customer, maintainer, third parties, or infrastructure.

4. Example Reference Standards & Materials

4.1 Rail Safety

a) CSM-REA — Common Safety Method for Risk Evaluation and Assessment

Commission Implementing Regulation (EU) No 402/2013
Link: https://www.legislation.gov.uk/eur/2013/402/contents

b) ROGS — Railways and Other Guided Transport Systems (Safety) Regulations 2006

Link: https://www.legislation.gov.uk/uksi/2006/599/contents

c) Technical Specifications for Interoperability (TSIs)

ERA overview:
Link: https://www.era.europa.eu/domains/technical-specifications-interoperability_en

d) UK NTSNs (TSI equivalent) — Department for Transport
https://www.gov.uk/government/collections/rail-interoperability-national-technical-specification-notices-ntsns

4.2 Cybersecurity and Information Security

a) BS EN ISO/IEC 27001 – Information Security Management Systems

Link (ISO): https://www.iso.org/standard/27001

b) Cyber Essentials Plus (UK Government Scheme)

Link (NCSC): https://www.ncsc.gov.uk/cyberessentials/overview

c) IEC/ISA 62443 Series – Industrial / OT Cybersecurity

ISA official:
Link: https://www.isa.org/standards-and-publications/isa-standards/isa-iec-62443-series-of-standards

d) IEC 63452 – Railway Applications – Cybersecurity – (to be published 2026)

BSI Development Timeline:
Link: https://standardsdevelopment.bsigroup.com/projects/2022-01003

e) PD CLC/TS 50701 – Railway Applications – Cybersecurity

Link: https://standardsdevelopment.bsigroup.com/projects/2022-00039

f) ISO/IEC 29147 – Vulnerability Disclosure

Link (ISO): https://www.iso.org/standard/72311.html

g) ISO/IEC 30111 – Vulnerability Handling Processes

Link (ISO): https://www.iso.org/standard/69725.html

h) ISO/IEC 62402 – Obsolescence Management

Link (IEC): https://webstore.iec.ch/en/publication/59531

4.3 Railway Safety and Software Development

a) BS EN 50126 – RAMS (Reliability, Availability, Maintainability, Safety)

Link (BSI): Part 1 : https://knowledge.bsigroup.com/products/railway-applications-the-specification-and-demonstration-of-reliability-availability-maintainability-and-safety-rams-generic-rams-process-1

Part 2: https://knowledge.bsigroup.com/products/railway-applications-the-specification-and-demonstration-of-reliability-availability-maintainability-and-safety-rams-systems-approach-to-safety-1

b) BS EN 50129 – Safety related electronic systems for signalling

Link (BSI): https://knowledge.bsigroup.com/products/railway-applications-communication-signalling-and-processing-systems-safety-related-electronic-systems-for-signalling-1

c) BS EN 50159 – Safety related communications

Link (BSI): https://knowledge.bsigroup.com/products/railway-applications-communication-signalling-and-processing-systems-safety-related-communication-in-transmission-systems-1

d) BS EN 50716 – Railway Applications – Requirements for Software Development

Link (BSI): https://standardsdevelopment.bsigroup.com/projects/2022-00241

e) BS EN 50128 / BS EN 50657 (now superseded by EN 50716 above)

Link: BSI catalogue.
Referenced in EN 50716 context per search output.

f) BS EN 61375 – Train Communication Network

Link (BSI): https://landingpage.bsigroup.com/LandingPage/Series?UPI=BS%20EN%2061375

g) RIS-2700-RST — Verification of Engineering Change to Rail Vehicles (RSSB)

RSSB publications site:
Link: https://www.rssb.co.uk/standards-catalogue/CatalogueItem/ris-2700-rst-iss-2

4.4 UK Data Protection Regulations & Cyber Regulations

a) Data Protection Act 2018 / UK GDPR

Link: https://www.legislation.gov.uk/ukpga/2018/12/contents

b) Privacy and Electronic Communications Regulations (PECR) 2003

Link: https://www.legislation.gov.uk/uksi/2003/2426/contents

c) Computer Misuse Act 1990

Link: https://www.legislation.gov.uk/ukpga/1990/18

d) Network and Information Systems Regulations 2018 (NIS)

Link: https://www.legislation.gov.uk/uksi/2018/506/contents

e) Cyber Security Resilience Bill 2025

(Parliament tracking page – Royal Assent in 2026)
Link: https://bills.parliament.uk/bills/4035

4.5 Further Resources

a) NCSC Software Security Code of Practice

Link: https://www.ncsc.gov.uk/section/software-security-code-of-practice/overview

5. Definitions

Purpose
This annex defines key terms used throughout the Guidance. Definitions are aligned with IEC 62443, IEC 63452, PD CLC/TS 50701, BS EN standards, UK regulatory terminology, and common rail operational technology practice.

5.1 Organisational Roles & Parties

Contracting Authority (CA)

The public body responsible for preparing the procurement, issuing the ITT, evaluating bids, awarding the contract, and ensuring requirements are met throughout the asset lifecycle.

Customer

The organisation procuring and operating the rolling stock, responsible for system ownership, governance, and regulatory compliance (e.g., NIS Regulations, ROGS).

Supplier

Any organisation responsible for designing, developing, integrating, delivering, commissioning, or supporting rolling-stock systems or subsystems.

Maintainer

The party responsible for maintenance activities, including scheduled maintenance, corrective repairs, configuration updates, and application of cyber security controls or patches as agreed in the TSA.

ROSCO (Rolling Stock Company)

Asset owner leasing rolling stock to operators. May hold responsibilities for configuration control, assurance, or upgrades depending on contractual arrangements.

Operator

The Train Operating Company (TOC) or passenger service operator responsible for service delivery and operational use of the rolling stock.

Third-party Assessor

An independent organisation conducting cyber security assessment, V&V activities, penetration testing, or assurance in accordance with accepted standards.

5.2 Systems, Architecture & Assets

Asset

Any hardware, software, configuration item, interface, data store, network segment, or operational tool forming part of or interacting with the rolling-stock system.

Subsystem

A distinct functional group of components (e.g., TCMS, ETCS, HVAC, CCTV, diagnostics), typically forming a security zone.

Zone

A group of assets with common security characteristics or trust boundaries, as defined in IEC 62443 and IEC 63452.

Conduit

A controlled communication channel between zones, subject to routing, filtering, or other security controls.

Configuration Item (CI)

Any element whose configuration state must be controlled to maintain security (hardware, software, firmware, parameters, rules, certificates, keys).

Modification State (Mod State)

The current configuration of a hardware component including firmware versions, replaced parts, and deviations from original build.

Network Boundary

A point where a subsystem or zone interfaces with another system, network, or external environment, requiring security controls.

Diagnostics / Wayside Systems

Offboard systems that support maintenance, configuration upload/download, monitoring, or analysis of rolling-stock systems.

5.3 Security Levels, Risk, and Assurance Concepts

Security Level (SL)

A target cyber security capability derived from IEC 62443-3-3 or IEC 63452 representing the level of protection required against defined threat actors.

Capability Security Level (CSL)

The level of security realistically achieved by a subsystem based on its design, constraints, and supplier capability. CSL must be compared to SL and justified where gaps exist.

Risk Assessment

A structured evaluation of threats, vulnerabilities, impacts, and likelihoods aligned to IEC 62443/IEC 63452, informed by system context and operational exposure.

Assurance

Evidence based activities demonstrating that cyber security requirements have been met, including documented arguments, testing, and lifecycle controls.

Assurance Regime

The combination of Supplier, Customer, and third-party security assessment activities (plan, responsibilities, documentation, V&V, acceptance gates).

Verification and Validation (V&V)

Verification checks whether requirements have been met; validation ensures the system satisfies operational needs. May be Supplier led or independently assured.

Cyber Security Acceptance Gate

A contractual checkpoint requiring delivery and acceptance of specific cyber artefacts or evidence before proceeding to the next project phase.

Cyber Security Case (CSC)

A structured argument, following IEC 63452 or PD CLC/TS 50701, demonstrating the asset is acceptably secure based on evidence, risk assessments, testing, and lifecycle controls.

Cyber Security Management Plan (CSMP)

The Supplier owned lifecycle governance document detailing responsibilities, processes, controls, monitoring, and update strategy for each system.

5.4 Bills of Materials & Configuration Transparency

SBOM (Software Bill of Materials)

A machine readable inventory of all software components, dependencies, versions, provenance, and known vulnerabilities.

HBOM (Hardware Bill of Materials)

A structured list of all hardware components, sub-assemblies, firmware versions, and modification states.

SBOM/HBOM Delta

A change set highlighting new vulnerabilities, replaced components, updated versions, or deviations from previous BOM versions.

Tamper Evident Delivery

A mechanism ensuring integrity of delivered artefacts (digital signatures, hashes, secure file transfer with verification).

Secure Handling Process (for SBOM/HBOM)

Jointly agreed procedures defining storage, access control, audit logging, encryption, and circulation limits due to sensitivity.

5.5 Monitoring, Detection & Incident Concepts

Monitoring

Continuous or periodic observation of logs, network traffic, telemetry, system behaviour, or alerts to detect anomalies or cyber threats.

Intrusion Detection System (IDS)

A system detecting unauthorised or abnormal activity using signatures, heuristics, or behavioural methods.

Monitoring Data Sources

Logs, network captures, configuration changes, security events, and telemetric data collected for security assurance.

Alerting and Escalation

Defined triggers, severity levels, and communication pathways ensuring security incidents are reported to responsible personnel.

Incident

Any confirmed or suspected cyber event that compromises or threatens confidentiality, integrity, availability, or safety of the system.

Incident Response

Actions taken to investigate, contain, mitigate, recover from, and learn from cyber incidents.

Containment

Immediate steps to isolate compromised systems, remove access, disable channels, or limit threat propagation.

5.6 Testing, Validation & Updates

White-Box Penetration Test

A penetration test performed with full system knowledge (architecture, design, code, credentials) to simulate an informed attacker.

Revalidation Trigger

Any change (software, firmware, architecture, configuration, interface) that materially alters the risk posture and requires re-testing.

Patch Management

Processes governing identification, testing, approval, and deployment of security patches or updates.

Obsolescence Management

Activities ensuring ongoing support for components over time, including notice of end of support and arrangements for continued security maintenance.

Source Code Escrow

A legally managed repository of source code or build artefacts, released to the Customer under defined conditions (e.g., Supplier insolvency).

5.7 Access, Identity & Maintenance

Access Control

Technical and procedural measures enabling authorised access while preventing unauthorised access (RBAC, least privilege, MFA).

Privileged Access

Access granting elevated rights (admin, root, engineering access). May be pre-handover (Supplier) or post-handover (TSA defined).

Multifactor Authentication (MFA)

Authentication requiring two or more independent credentials (e.g., password + device token + certificate).

Secure Maintenance Regime

A structured approach ensuring maintenance activities are conducted securely, using controlled tools, credentials, and processes.

Technical Service Agreement (TSA)

A multi-party agreement defining responsibilities for support, updates, monitoring, access, and secure maintenance throughout the lifecycle.

5.8 Safety, Regulation & Interactions

Safety Case

The documented demonstration that the system is acceptably safe for operation under defined conditions.

Cyber–Safety Hazard

Any cyber vulnerability or compromise with the potential to affect safety, operational performance, or regulatory compliance.

CSM-REA (Common Safety Method – Risk Evaluation & Assessment)

EU/UK aligned method for assessing rail safety risks, requiring identification, control, and validation of hazards (including cyber).

Cyber–Safety Traceability Matrix

A mapping from hazards → cyber risks → controls → SLs → evidence → CSC/Safety Case references.

Change Control Board (CCB)

A multi-party governance forum assessing changes that impact safety or cyber security, required before applying updates.

5.9 Procurement, Governance & Documentation

Invitation to Tender (ITT)

The formal procurement document issued by the CA defining requirements, evaluation criteria, deliverables, and contractual expectations.

Bidder Response

All evidence, documentation, and commitments submitted by a Supplier in response to the ITT.

Evaluation Framework

The CA developed structure used to assess bid completeness, compliance, merit, and traceability.

Requirement Traceability

The ability to link each requirement in the ITT to corresponding Supplier evidence, assessment criteria, and acceptance decisions.

Deviation

A Supplier's proposal not meeting the stated requirement, accompanied by justification and compensating controls.

Assumption

A statement made by the Supplier about scope, responsibilities, or conditions upon which the bid is based.

Dependency

A condition, resource, or action required from the Customer, maintainer, operator, ROSCO, or third parties for security controls to be effective.

5.10 Miscellaneous Technical Terms

Threat

Any circumstance or actor with the potential to exploit a vulnerability.

Vulnerability

A weakness in design, implementation, configuration, or process that could be exploited.

Casual Vulnerability

A vulnerability that is easily exploitable using simple tools or low expertise, requiring priority remediation.

Data at Rest / Data in Transit

Stored data / transmitted data requiring encryption and protection per applicable standards.

Time Synchronisation (e.g., NTP, GNSS)

The process ensuring log timestamps and event records remain accurate for monitoring, correlation, and forensics.

Secure Transmission

Use of cryptographically protected channels (e.g., TLS 1.2+, certificates, encryption) for sending data.