TEAM MANDATORY-ISH

ONE NETWORK, ONE STANDARD

Cyber Security Harmonisation for Australian Rail

ARiSO
AUSTRALIAN RAIL INDUSTRY STANDARDS ORGANISATION

EXECUTIVE SUMMARY

Australia's rail network is undergoing rapid digital transformation, with increasing reliance on interconnected operational technologies, advanced signalling, and data-driven systems. While this evolution is enabling improvements in safety, efficiency and interoperability, it is also exposing the network to an escalating cyber threat landscape—one that is becoming more frequent, targeted, and capable of impacting safety-critical operations.

Despite this shift, cyber security across the Australian rail industry remains fragmented. Rail operators and infrastructure managers currently rely on a combination of international frameworks, jurisdictional policies, and internal controls, resulting in inconsistent application, duplicated effort, and uneven levels of cyber maturity across the national network. In a vertically separated railway environment—where rolling stock and infrastructure regularly interact across jurisdictions—this lack of a unified approach creates systemic risk and challenges to interoperability.

This report identifies the adoption of a nationally harmonised rail cyber security standard, based on an uplifted version of AS 7770, as a critical enabler for a safer, more resilient, and interoperable rail network.
AS 7770 provides an established, rail-specific governance framework; however, in its current form, it remains high-level and non-prescriptive, limiting its effectiveness as a consistent and auditable national standard. In contrast, international standards such as IEC 62443 provide detailed, testable requirements for operational technology cyber security, but lack alignment with the unique characteristics of the Australian rail environment—particularly vertical separation, shared risk ownership, and safety integration.

This report proposes a hybrid approach, positioning a modernised AS 7770 as a nationally adopted "umbrella" standard, supported by aligned integration with IEC 62443 (and, in time, IEC 63452). This model would:

- Establish a consistent national baseline for cyber security
- Enable trusted interoperability between rolling stock and infrastructure across jurisdictions
- Support the safe implementation of Digital Train Control (DTC) and European Train Control System (ETCS)
- Improve regulatory alignment and sector-wide risk visibility
- Simplify procurement, supplier assurance, and lifecycle management

The report identifies key uplift areas required to transition AS 7770 from a principles-based framework to an effective national standard, including:

- Introducing prescriptive and assessable requirements
- Strengthening lifecycle assurance and evidence requirements
- Clarifying roles, responsibilities and supplier obligations

While the benefits of harmonisation are significant, the report also acknowledges implementation challenges, including cost, capability gaps, legacy system constraints and the need to integrate cyber security within existing safety and regulatory frameworks. A tiered, risk-based implementation approach, supported by shared industry capability and governance through ARISO, ONRSR, and national coordination bodies, is proposed to address these challenges.

Ultimately, this report concludes that cyber security must be treated not as a standalone IT function, but as a core component of rail safety, interoperability, and national resilience. A harmonised, rail-specific cyber security standard is essential to underpin Australia's transition to a digitally enabled rail network and to ensure that the benefits of modernisation are not undermined by avoidable systemic risk.

DISCLAIMER

Images included in this report have been generated using AI (Artificial Intelligence) and are provided for illustrative and decorative purposes only. They should not be interpreted as factual representations of real-world systems, assets or locations.

Abbreviation	Definition
ARISO	Australian Rail Industry Standards Organisation
ARTC	Australian Rail Track Corporation
ACSC	Australian Cyber Security Centre
ASD	Australian Signals Directorate
DTC	Digital Train Control
ETCS	European Train Control System
IACS	Industrial Automation Control Systems
IEC	International Electrotechnical Commission
ITMM	Infrastructure and Transport Ministers' Meetings
ITSOC	Infrastructure and Transport Senior Officials Committee
IT	Information Technology
NIST	National Institute of Standards and Technology
ONRSR	Office of the National Rail Safety Regulator
OT	Operational Technology
SOCI Act	Security of Critical Infrastructure Act 2018
TfNSW	Transport for New South Wales

CONTENTS

1.0 INTRODUCTION

The Australian rail network is undergoing rapid digital transformation, with increasing reliance on interconnected operational technologies, intelligent transport systems, cloud-based platforms, and data-driven asset management and monitoring. These advancements support the Australian rail industry's move towards an interoperable and intelligent operational railway network by delivering benefits for safety, operational efficiency, network performance and passenger experience.

With modernisation and increasing reliance on integrated digital systems to support the rail network, exposure to cyber security threats will increase. The Australian Signals Directorate (ASD) and Australian Cyber Security Centre (ASCS) responded to more than 1,200 cyber security incidents in 2024-25, with critical infrastructure, including transport, representing 13% of all incidents (ASD/ACSC Cyber Threat Report). The trend is expected to increase each year with cyber attacks becoming more frequent, targeted and automated.

Research forecasts that the Australian railway cyber security market will grow from approximately USD $228 million in 2025 to almost USD $577 million by 2033 (Grand View Research). This is to combat key rail network systems (e.g., signalling systems, communication networks, rolling stock etc.) that may be susceptible to malicious actors and targeted cyber security attacks.

Australia's rail networks face a number of unique cyber security challenges such as:

- Rail network signalling systems, train control methods, and safeworking rules vary across States
- Rail systems often comprise legacy infrastructure that was not originally designed to accommodate modern cyber security protections
- Rail Transport Operators (RTOs) and Rail Infrastructure Managers (RIMs) manage geographically dispersed assets and operational and maintenance requirements may vary across States
- The long operational lifespan of rail assets can create challenges in maintaining software support, system upgrades, and ongoing cyber security assurance.

It is therefore important for the Australian rail industry to establish a consistent, industry specific framework and approach for managing cyber security risks.

Unique Cyber Security Challenges Facing Australia's Rail Networks

	Challenge	Rail context	Why it matters
1	**Variation across states**	Signalling systems, train control methods and safeworking rules vary across jurisdictions.	Creates inconsistent cyber expectations and interface risk.
2	**Legacy infrastructure**	Rail systems often comprise legacy infrastructure not originally designed for modern cyber security protections.	Makes retrofitting controls complex and potentially disruptive.
3	**Dispersed assets and operations**	RTOs and RIMs manage geographically dispersed assets with differing operational and maintenance requirements.	Increases complexity in monitoring, response and assurance.
4	**Long asset lifecycles**	Rail assets operate for long periods, which can exceed typical software support and upgrade cycles.	Challenges ongoing patching, upgrades and cyber assurance.

It is therefore important for the Australian rail industry to establish a consistent, industry-specific framework and approach for managing cyber security risks.

1.1 REPORT PURPOSE

The purpose of this report is to outline the case for the adoption of AS 7770:2018 Rail Cyber Security which is currently a non-mandatory standard. This report outlines:

- The benefits to the Australian rail industry for implementing AS 7770 at a national level
- Interface with digital train control (DTC) implementation
- Alignment of AS 7770 with key international cyber security standards such as IEC 62443 and IEC 63452
- Challenges and risks with mandating AS 7770 at a national level, including governance considerations

2.0 INDUSTRY ANALYSIS

A harmonised cyber security standard would give the Australian rail industry a unified, interoperable, and resilient foundation for managing cyber risk across a network that is increasingly digital and nationally interconnected. Today, rail operators and infrastructure managers work within a patchwork of frameworks—ISO 27001, NIST CSF, state-based requirements, and bespoke organisational controls. This fragmentation creates inconsistent expectations, duplicated compliance effort, and uneven cyber maturity across jurisdictions.

A single, nationally aligned standard would streamline these differences and ensure that systems, data, and operational technologies can interact securely across state borders. It would reduce friction for operators that interface with multiple networks, simplify procurement for suppliers, and give regulators a clearer view of sector-wide risk. Harmonisation also strengthens national resilience by enabling consistent incident response processes, shared terminology, and coordinated cross-jurisdictional recovery when cyber events occur.

As the sector adopts advanced signalling, automation, IoT-enabled assets, and integrated mobility platforms, a common cyber baseline becomes even more critical. It provides clarity for vendors, confidence for investment, and a stable platform for digital transformation. Ultimately, a harmonised cyber security standard is a strategic enabler: it reduces systemic risk, supports interoperability, and positions the Australian rail industry for a safer and more connected future.

INDUSTRY SNAPSHOT

Australian Rail Track Corporation (ARTC)

ARTC doesn't have a single externally validated cyber security standard that is certified against. Instead, ARTC draws on:

- NIST and the ASD Essential Eight for general guidance
- The ISM where applicable for technical controls
- SOCI obligations for critical infrastructure compliance
- Elements of ISO 27001 for governance and risk management

In this context, AS7770 is broadly consistent with the approach taken by ARTC, but is not the primary driver of controls. A harmonised cyber security standard which incorporates more actionable guidance (drawing upon IEC 62443, with future alignment to IEC 63452) would provide greater clarity and consistency. AS7770 remains a sensible standard to endorse, particularly with a view to updating and strengthening it, as opposed to being a complete solution. The future value will likely come from acting as a rail-specific umbrella that clearly aligns to more detailed cyber standards, especially as ETCS becomes more prevalent nationally.

Transport for New South Wales (TfNSW)

TfNSW maintains a structured and mature cyber security posture tailored to the specific requirements of their OT environments.

TfNSW has developed a suite of internal cyber security standards aligned with internationally recognised frameworks, particularly IEC 62443 with some variation in its application. This alignment ensures that industrial control system security requirements are implemented in accordance with global best practice, while being adapted to the operational constraints and safety-critical nature of railway systems.

In line with obligations under the SOCI Act, TfNSW has identified its critical infrastructure assets, which are subject to targeted cyber security assessment due to their importance to the safe and reliable operation of the rail network.

TfNSW has also assessed the applicability of the ACSC Essential Eight and determined that, while effective for enterprise IT environments, it is not fully suitable for OT systems. This is due to differing operational constraints, legacy system considerations, and availability requirements. In response, TfNSW has developed an alternative control framework known as the OT10, specifically tailored to manage OT cyber security risks while maintaining operational continuity and safety.

Cyber security is embedded within TfNSW's engineering and assurance processes. Cyber risks are systematically considered at both enterprise and project levels, with dedicated cyber security assessments undertaken where appropriate. Requirements are incorporated early in the project lifecycle, typically from concept and design, and maintained through delivery and integration. This ensures that cyber security is designed into systems from the outset and actively managed throughout the lifecycle. However, in practice TfNSW continues to see gaps and challenges remain in retrofitting cyber security controls into legacy systems.

Queensland Government

From a Queensland perspective, cyber security is primarily governed through a whole of government policy framework rather than rail specific standards. Information and cyber security requirements are defined under the Queensland Government Information Security Policy (IS18), which applies broadly across agencies and functions.

IS18 mandates the establishment of an Information Security Management System aligned to ISO 27001, providing a structured, risk-based approach to managing cyber security. In addition, agencies are required to implement the Australian Signals Directorate (ASD) Essential Eight mitigation strategies.

Queensland has developed a number of jurisdiction-specific frameworks and guidance materials, including the Queensland Government Information Security Classification Framework (QGISCF), the Digital Enterprise Standard (DES), and the Queensland Government Architecture Framework (QGAF). These artefacts provide additional structure and consistency for implementing cyber security controls across government environments.

Queensland's approach reflects a broader enterprise IT-centric model, with cyber controls derived from general government policy and adapted within individual agencies. While this provides a consistent governance baseline, it may result in variability in how cyber security is interpreted and applied within operational technology and safety-critical rail contexts.

3.0 STANDARD SELECTED - AS 7770

Overview of AS7770

AS 7770 is ARISO's established framework for managing cyber risks within the Australian Rail Industry. Its purpose is to preserve the reliability, availability, maintainability, and safety of rail control systems, while also protecting the accuracy and privacy of information stored in ancillary systems. Rather than acting as a rigid, technically enforceable cyber security standard, AS7770 provides a high-level governance framework. The current 2018 version aligns with how RTOs and Rail Infrastructure Managers (RIMs) should think about cyber risk in rail, but in practice, other frameworks are used, which provide more actionable guidance. This non-prescriptive, principles-based approach is intended to facilitate a broad range of applications across the industry, especially given the varied technical maturity among different organisations.

National Alignment and the Role of ARISO

While the core principles of AS 7770 remain sound, the national shift toward DTC makes an update necessary. Therefore, the position taken is to adopt a modernised version of AS7770 as a nationally harmonised standard. The proposed variations would see AS7770 become a foundation, from which more prescriptive standards can be easily applied. Historically, voluntary adoption of cyber security standards in railways has led to inconsistent security levels and practices across different networks and operators. By nationally aligning to this standard, ARISO can ensure a baseline level of cyber security, which would be greatly beneficial as DTC becomes the norm and with ETCS as the technology of choice for the NNI. Furthermore, a nationally harmonised baseline would be greatly beneficial to interoperability, especially in a vertically separated railway such as that of Australia. A single trip may involve crossing multiple interfaces, which becomes significantly more difficult if different security levels could be maintained by each rolling stock operator and RIM.

International Alignment: IEC 62443 & IEC 63452

IEC 62443 is an internationally recognised operational technology cyber security standard. It provides a comprehensive, actionable framework for risk management, lifecycle controls, safety constraints, operational practices and roles and responsibilities. As the scope of the standard is broadly set as Operational Technology (OT), the standard has been written in a modular, role based way, which allows users to select only the parts which are relevant to their responsibilities, or the stage of the system lifecycle that is being worked with.

Furthermore, it has been written with local regulatory requirements in mind, making advice applicable to Australian asset owners and operators, which is critical for alignment within the rail industry. Standards Australia has already adopted IEC 62443 as national standards for protecting OT in critical infrastructure, so any updates made to AS7770 should ensure alignment where possible, to avoid duplication, or interpretation effort (Standards Australia, 2025).

The upcoming standard, IEC 63452 is being written as an international cybersecurity standard for railway cyber security. It has a wide scope of application applying to mainline, metro, trams, freight, fully automated systems and rolling stock and fixed installations. Critically, it also builds on IEC 62443 for risk management, roles and lifecycle controls, safety constraints and operational practices (Kambourian, 2026).

This standard however, is poised to be highly prescriptive and technically demanding, which presents a challenge for national adoption, given the varied capital expenditure available for cyber security among both below and above rail operators.

While IEC 62443 (and likely once released, IEC 63452) provide a robust technical framework for system lifecycle security, it exhibits distinct structural gaps when applied to the realities of the Australian rail landscape. The most significant of these gaps is vertical separation, especially when considering Australia's regional and interstate railway lines. In this vertically separated model, a single train journey crosses multiple complex interfaces, managed by different RIMs. Conversely, each RIM aims to accept as much rolling stock as possible, so far as is reasonably practical. The current IEC standards treat systems with a degree of technical isolation that fails to address the shifting boundaries of liability and risk ownership that occur when an asset moves between disparate network environments.

There is little to no doubt that once released, IEC 63452 will become a critical standard for cyber security in the Australian rail industry, but to increase adoption, and cover the specific gaps presented by the Australian rail industry, a translational piece is required, and this is the suggested gap to be filled by a nationally harmonised, updated version of AS7770, which should implement the suitable, modular pieces of IEC 62443, so far as far as is reasonably practical for national implementation, but crucially, it must consider Australia's unique issue of vertical separation.

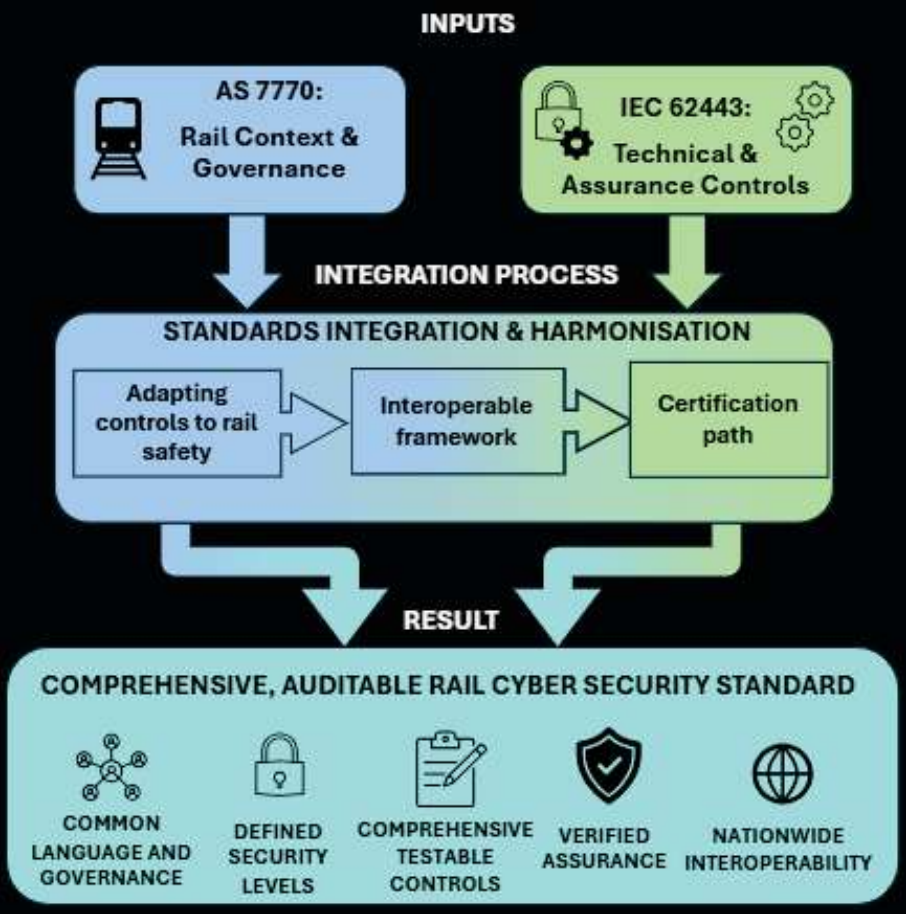

Figure 1: Standards harmonisation flow

4.0 GAPS OF AS 7770

AS 7770 is a high level, principles based cyber security standard intended to establish governance expectations and a common language for cyber security in rail systems. It does not prescribe technical security controls, define security levels, or provide testable or certifiable requirements. Its role is therefore strategic and framework level, rather than engineering or assurance focused.

While AS 7770 is rail focused, it lacks several elements required of a nationwide, mandatory, and interoperable cyber security standard. By comparison, the IEC 62443 series define how OT/Industrial Automation Control Systems (IACS) cyber security is governed, designed, built, operated, and assured. It establishes supplier obligations for secure development and maintenance, defines risk assessment processes, provides normative and testable security requirements, defines security levels, and supports auditable and certifiable assurance.

IEC 62443 has been widely adopted to protect critical infrastructure and has provided valuable guidance in achieving and maintaining cyber secure OT systems. However, it also falls short when applied directly to railway environments with an interoperability objective. In particular:

- It is not rail specific.
- It does not explicitly integrate with railway safety standards, focusing on cyber risk rather than safety risk and treating safety as an external consideration.
- It assumes a single asset owner or security authority and does not define trust relationships between independent rail operators.

Addressing the gaps between AS 7770 and IEC 62443 provides an opportunity to develop a rail focused cyber security standard that can establish trust between operators as rail vehicles operate across jurisdictions. Four key uplift areas are outlined below.

Prescriptive Requirements and Assessability

AS 7770 is a principles based, governance focused standard rather than a standard that can be audited for technical conformance. While this approach provides flexibility, it also leads to variable interpretation and inconsistent implementation across rail operators and maintainers, limiting the ability to conduct consistent and objective assessments of cyber security controls.

By contrast, IEC 62443 provides a modular set of normative, testable requirements covering asset owners, service providers, system integrators, and product suppliers AS7770 would benefit from an uplift to include prescriptive requirements to support consistent application of cyber security across rail networks and reduce variability driven by local interpretations of risk based design. This would make assurance and interoperability discussions more concrete and evidence based, rather than subjective.

Defining minimum security target levels for each zone would further support interoperability between jurisdictions. Cyber security across interconnected rail networks is only as strong as the weakest link, therefore, establishing agreed minimum levels and ensuring that each jurisdiction meets and accepts those minimums, would increase trust and support smoother operational transitions between networks.

Lifecycle Coverage

AS 7770 establishes that cyber security must be addressed across the full system lifecycle, however, it

provides limited guidance on specific lifecycle deliverables, handover artefacts, and assurance evidence needed to make this standard operationally effective at a national level. By comparison, IEC 62443 defines explicit lifecycle expectations, including secure system design risk assessment, secure product development lifecycles, defined operational processes, and clear evidence requirements at each lifecycle stage.

This is particularly evident in operational contexts where cyber threats evolve rapidly while rail safety approval and change processes are necessarily conservative. As a result, activities such as patching, vulnerability remediation, and security upgrades can introduce significant challenges and complexity within existing approval frameworks. AS 7770 would benefit from clearer lifecycle requirements covering vulnerability management, patch governance, change impact assessment, and guidance on how cyber security evidence is managed alongside safety assurance evidence, including the interface between a Cybersecurity Case and the Safety Case.

Zones and Conduits

AS 7770 currently requires logical and physical segregation of rail systems based on safety impact, however, it does not define a formal zone and conduit model, leaving cyber boundaries and interface controls largely undefined. In comparison, IEC 62443 formalises segregation through a zones and conduits methodology and provides structured documentation and interface control expectations. However, IEC 62443 does not use safety impacts as a primary factor in determining segregation, which is a key consideration for railway system design and assurance.

Uplifting AS 7770 to adopt a standardised zoning and conduit methodology combined with segregation by safety impact and minimum expectations for common rail architectures (i.e. field systems, onboard systems, control centres, and corporate interfaces) would significantly strengthen the standard. This would shift AS 7770 from a predominantly principles-based framework to a more consistent, auditable and interoperable rail cyber safety framework.

Standardising zones and conduits would remove the need for each railway network or project to define its own cyber boundary model. A shared architectural baseline would improve clarity and efficiency in design, procurement, assurance, and regulatory engagement, while still allowing risk based tailoring where justified.

Roles, Responsibilities and Supplier Assurance

AS 7770 is written primarily for RTOs, placing responsibility for cyber security governance and assurance with the asset owner, while expecting suppliers and contractors to be aware of applicable requirements. However, it does not clearly define lifecycle roles, responsibilities, or deliverables across asset owners, system integrators, and service providers.

IEC 62443 explicitly separates responsibilities through distinct requirement sets for asset owner security management systems (IEC 62443-2-1) and service provider security programs (IEC 62443-2-4), supported by a clearer contractual and deliverables based model. While AS 7770 references IEC 62443-2-4 as a useful procurement mechanism, this separation is not explicitly defined within the standard.

Strengthening AS 7770 by clarifying lifecycle responsibilities and introducing standardised supplier and integrator requirements would improve supplier assurance and procurement enforceability. Although AS 7770 already expects supply chain information sharing and contractual inclusion of cyber security requirements, it does not define these expectations in a consistent or auditable way. Defining requirements for vulnerability disclosure, security updates, and evidence provision would strengthen supplier accountability and make ‘secure by design’ outcomes demonstrable.

5.0 BENEFITS AND RISKS

The adoption of a nationally harmonised and uplifted rail cyber security standard, based on an enhanced AS 7770 and aligned with international standards such as IEC 62443, presents a significant opportunity for the Australian rail sector to improve its cyber resilience, interoperability and long term sustainability. However, these benefits must be balanced against a range of implementation and integration risks that require careful consideration.

Benefits and Opportunities

	Benefit / opportunity	Description
1	**Consistent application of cyber security across the national network**	A harmonised standard establishes a common baseline for cyber security controls across all jurisdictions. This reduces fragmentation and ensures that cyber risks are managed in a consistent manner.
2	**Improved interoperability between rail networks and operators**	Interoperability is a critical objective of national rail reform. A standardised approach to cyber security supports trusted interactions between rolling stock and infrastructure as assets transition across jurisdictional boundaries. This is particularly important in Australia's vertically separated rail model, where multiple operators and infrastructure managers must exchange data and maintain assurance over system integrity. Establishing agreed minimum security levels reduces uncertainty at interfaces and enables more efficient cross-network operations.
3	**Support for Digital Train Control (DTC) and ETCS implementation**	The transition toward Digital Train Control and the adoption of ETCS as the national platform introduces increasingly connected, data-driven, and software-dependent systems. A nationally aligned cyber security standard provides a stable and consistent foundation to support this transformation, ensuring that cyber risks are considered alongside safety, reliability, and performance requirements.
4	**Enhanced risk management and regulatory alignment**	A national standard enables a consistent approach to cyber risk identification, assessment, and treatment across the rail sector. This improves transparency for regulators and supports alignment with obligations such as the SOCI Act. It also enables clearer integration of cyber security into safety management systems, supporting a more holistic approach to managing operational risk.
5	**Reduced complexity in procurement and supplier assurance**	Suppliers currently face varying cyber security requirements across different rail organisations, leading to inefficient procurement processes and inconsistent assurance expectations. A harmonised standard simplifies this by defining a common set of requirements for system integrators, equipment suppliers, and service providers. This improves supply chain transparency, reduces duplication of assurance activities, and supports more effective "secure-by-design" outcomes.
6	**Stronger industry capability and knowledge sharing**	A unified standard provides a common language and framework for cyber security across the industry, enabling greater collaboration and knowledge sharing between operators, the regulator and suppliers. It supports the development of shared tools, assessment methodologies, and training programs, helping to address the current cyber security skills gap within the rail sector.
7	**Alignment with international best practice while maintaining local relevance**	Positioning an uplifted AS 7770 as a rail-specific umbrella standard allows Australia to align with international frameworks such as IEC 62443 while addressing unique national challenges, including vertical separation, legacy systems, and varying organisational maturity. This approach enables global consistency without compromising applicability to the Australian rail context.

Risks

	Risk	Description
1	**Implementation cost and resource burden**	The adoption of a nationally aligned standard may introduce additional costs for operators, particularly those with lower levels of cyber maturity or extensive legacy infrastructure. Investment may be required in governance processes, system upgrades, and assurance activities. Without a proportionate implementation model, this could create barriers to adoption across smaller or regional operators.
2	**Variation in organisational maturity and capability**	Rail organisations operate at different levels of cyber security maturity and technical capability. A prescriptive or poorly tailored standard could be difficult for some organisations to implement effectively, leading to inconsistent outcomes or superficial compliance rather than meaningful risk reduction.
3	**Integration with existing safety and operational frameworks**	Cyber security must be integrated into established rail safety and assurance processes. If not carefully aligned, there is a risk that cyber requirements may be treated as a separate compliance activity. This separation can result in poorly coordinated implementation of controls, which may unintentionally impact system safety, availability, and operational reliability.
4	**Transition challenges for legacy systems**	Many rail systems were not designed with modern cyber security requirements in mind. Retrofitting controls into these environments can be complex and may introduce unintended operational or safety impacts if not carefully managed.

6.0 INDUSTRY CHALLENGES

While AS 7770 provides a nationally recognised, rail-specific framework for managing cyber security risk, several structural and systemic challenges may limit its widespread adoption across the Australian rail industry (ARISO, 2018). These challenges are not unique to cyber security and reflect broader issues associated with implementing new standards across a diverse, multi-operator and safety-critical sector.

Cost and proportionality of implementation

A primary challenge for industry adoption of AS 7770 is the cost associated with implementation, particularly for smaller rail transport operators, infrastructure managers and heritage or regional rail networks. Although AS 7770 is principles-based rather than prescriptive, effective implementation typically requires investment in governance structures, cyber risk assessments, asset identification and assurance processes (ARISO, 2018).

Australian rail literature highlights that cyber security initiatives have historically competed with more visible safety, asset and operational priorities, particularly where cyber threats are perceived as indirect or unlikely to result in immediate operational harm (Rail Express, 2020). This creates a barrier where organisations struggle to justify expenditure without a clear regulatory mandate or demonstrable return on investment.

To address this, AS 7770 could be implemented using a tiered maturity model that defines baseline, intermediate, and advanced levels of cyber security capability. This model would operate above a defined set of minimum baseline security requirements necessary for interoperability between rail networks and ensure consistent trust between jurisdictions. While the tiered model enables proportionate uplift beyond this baseline based on organisational size, risk profile, and operational complexity. This approach aligns with the risk-based regulatory philosophy promoted by ONRSR, which encourages controls that are “reasonably practicable” rather than uniformly applied across all operators (ONRSR, 2023). A tiered model would allow smaller organisations to achieve baseline compliance while providing a structured pathway for maturity uplift over time.

Industry capability and cyber security skills gap

A further challenge is the uneven distribution of cyber security capability across the Australian rail industry. Larger operators may maintain dedicated cyber security or digital engineering functions, whereas smaller organisations often rely on generalist IT resources or external vendors with limited understanding of rail operational technology (OT) and safety-critical systems (Engineers Australia, 2025).

Rail cyber security requires expertise across IT, OT and safety domains, yet Australian research and industry forums consistently highlight a shortage of professionals with this combined skill set (Engineers Australia, 2025). This disparity risks inconsistent interpretation of AS 7770 and uneven levels of cyber maturity across the national rail network.

A practical solution is the development of shared industry capability, coordinated through ARISO and supported by Australian universities and professional bodies. This could include shared guidance material, rail-specific cyber risk assessment templates and access to independent cyber assessors with rail expertise. Academic engagement has already been demonstrated through Australian rail cyber security research and professional development programs, indicating that collaborative capability uplift is both feasible and scalable (Engineers Australia, 2025).

Legacy systems and variation in organisational maturity

The Australian rail network consists of organisations operating at significantly different levels of digital maturity, with many networks reliant on legacy systems designed before cyber threats were considered (ARISO, 2018). Retrofitting modern security controls into these environments can be complex, costly and, if poorly managed, introduce unintended operational or safety risks.

While AS 7770 intentionally avoids prescribing technical controls, this flexibility can create uncertainty for less mature organisations regarding where to prioritise effort and investment (ARISO, 2018).

To address this, ARISO could publish minimum viable cyber controls mapped directly to AS 7770 principles. These controls would focus on high-impact, low-disruption measures such as asset identification, access governance and incident response preparedness, enabling organisations to achieve meaningful risk reduction without requiring immediate replacement of legacy systems.

Integration with safety and regulatory frameworks

ONRSR guidance increasingly recognises the relationship between cyber security, system integrity and safe railway operations, particularly in the context of interoperability and networked systems (ONRSR, 2023). However, cyber security is not yet consistently embedded within rail safety management systems, assurance processes or regulatory reporting frameworks across the industry.

This separation reinforces the perception of cyber security as an IT responsibility rather than a contributor to operational safety risk.

Positioning AS 7770 explicitly within existing rail safety governance frameworks - such as change management, system assurance and incident investigation - would normalise cyber security as part of established safety practice. Australian rail industry analysis has highlighted the importance of integrating cyber risk into safety decision-making to ensure reliable and resilient rail operations (Rail Express, 2020).

In summary, while AS 7770 provides a robust foundation for managing cyber security risk in the Australian rail industry, its adoption is challenged by cost pressures, capability gaps, legacy infrastructure and the need for stronger integration with safety and regulatory frameworks. Through proportional adoption models, shared industry capability, targeted guidance and safety-led governance, these challenges can be addressed in a manner that supports achievable and sustainable nationwide adoption across rail organisations of all sizes.

7.0 GOVERNANCE

A harmonised Australian cyber security standard would deliver significant governance benefits for the Australian rail sector by creating a clearer and more consistent basis for cyber security decision-making.

This is increasingly important as rail operators navigate the introduction of DTC systems, critical infrastructure obligations, and the growing influence of international rail cyber frameworks such as IEC 62443.

Governance is the mechanism by which an uplifted AS 7770 goes from a technical standard to a nationally harmonised framework that supports interoperability, safety and productivity.

Notwithstanding the proposed benefits, the governance challenges are equally substantial;

Jurisdictional fragmentation

Australia's rail networks operate across multiple regulatory settings, with varying levels of maturity, risk appetite and operational priorities. Even where the value of harmonisation is accepted, agreeing on who sets the standard, who enforces it, and how compliance is demonstrated can be difficult.

Industry diversity

Freight, metropolitan, regional and light rail networks do not share the same technology base, safety context or resourcing capacity, so a single standard must be robust enough to provide national consistency while flexible enough to remain palatable to industry.

Accountability across shared environments

Cyber risk in rail is often distributed which can blur the lines between responsibility, incident response and assurance.

International alignment

Australia should aim to align any Australian harmonised standard with international approaches without creating unnecessary complexity or weakening local applicability.

Rate of change

Standards development, consultation and regulatory adoption are typically slower than the evolution of technology, so the governance model must support regular review, rapid updates and strong information-sharing across the sector.

Linkages to broader rail reform

A harmonised rail cyber security standard must remain connected to broader rail reform for interoperability – principally through the National Rail Action Plan (NRAP) and national coordination at ITMM.

The difference between generic 'railway cyber security' and 'European Train Control System (ETCS)' cyber security must also be considered. In 2025 Australian Transport Ministers selected ETCS as the technology of choice for the National Network for Interoperability, and as a result digital train control (DTC) has become a significant focus, , particularly ETCS (ITMM Communique, 11 Aug 2025). From a DTC perspective, the key considerations are likely to include whether the proposed standard is voluntary, harmonised or intended to be mandatory. This will enable industry to identify implementation costs, transition timing and treatment of legacy infrastructure and assets.

Governments will need to be the primary driver of national adoption of a harmonised rail standard. Because rail governance is shared across multiple levels of government, and cyber security risk management includes the supply chain and project organisations, a harmonised Standard is unlikely to achieve the intended national benefits without endorsement through ITMM/ITSOC and enforcement via a combination of ONRSR and the Security of Critical Infrastructure (SOCI) Act, administered by the Department of Home Affairs. Ultimately, Governments will be the decision point at which an uplifted AS7770 goes from a voluntary standard to a nationally endorsed harmonised standard.

As with all significant reforms, broad stakeholder engagement would be required via public consultation. Engagement should test whether proposed requirements support interoperability, are enforceable, proportionate across Australia's different rail contexts, how accountabilities are allocated, what implementation considerations are required, and what flexibilities may be needed e.g. a tiered maturity model.

Governance arrangements should clearly distinguish between policy setting, technical standard development, implementation responsibility and assurance. To ensure cyber security is integrated into rail reform rather than treated as a standalone exercise, a suitable model could build on existing national rail governance arrangements. Under this model, governments would provide policy endorsement and oversight through ITMM (with NTC support), while ARISO or a similar body would lead the technical development and ongoing maintenance of the standard, supported by specialist industry working groups. ONRSR and the Department of Home Affairs, in its role administering the SOCI Act, would determine how the standard is recognised within safety, regulatory or assurance frameworks. Operators and suppliers would remain responsible for implementing the standard within their own systems, contracts and risk controls.

A clear governance framework will also facilitate the development of a robust audit capability. Audit procedures should reflect the varied threat landscape of the rail environment, for example signalling systems, control centres or rolling stock interfaces. Enabling this capability through a clear governance framework and regulatory obligations will ensure that cyber security is part of rails continuous improvement cycle and not just a series of isolated exercises.

An example of how this could work in practice is included below at figure 2:

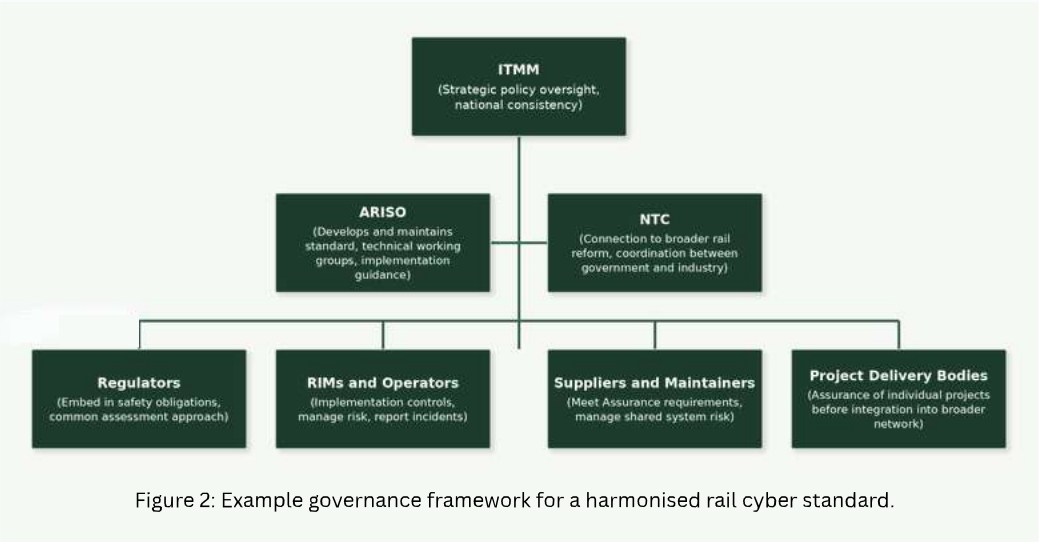

Figure 2: Example governance framework for a harmonised rail cyber standard.

Without clear governance, a harmonised standard risks becoming another guidance document; with clear governance, it becomes the mechanism for a nationally harmonised framework that supports interoperability, safety and productivity.

8.0 STRENGTHS, WEAKNESSES, OPPORTUNITIES AND THREATS OF A HARMONISED AS 7770

STRENGTHS

- Rail-specific framework with a strong governance foundation
- Establishes a common national baseline for cyber security
- Supports interoperability in a vertically separated railway
- Improves regulatory visibility and risk management consistency
- Simplifies procurement and supplier assurance

WEAKNESSES

- Inherent reliance on integration with external standards (IEC 62443 / future IEC 63452)
- Balancing prescriptiveness with industry flexibility
- Complexity of implementing a hybrid framework
- Potential duplication / overlap if alignment is not tightly managed

OPPORTUNITIES

- National interoperability and digital transformation
- Creation of a unified national cyber security ecosystem
- Strengthens national resilience and coordinated incident response
- Industry capability uplift and knowledge sharing
- Improves supply chain transparency and accountability
- Integration of cyber security into safety assurance

THREATS

- Implementation cost and resource burden
- Variation in industry maturity and capability
- Legacy system constraints
- Governance and jurisdictional fragmentation
- Integration challenges with safety and regulatory frameworks
- Rapid evolution of cyber threats vs slower standards development

9.0 CONCLUSION

The analysis in this report demonstrates that Australia's rail cyber security arrangements are not yet sufficiently consistent, mature or rail-specific to support the level of interoperability and digital integration now being pursued across the national network. While existing frameworks such as ISO 27001, NIST, the ASD Essential Eight, SOCI obligations and jurisdiction-specific policies provide useful cyber security guidance, they do not create a unified industry baseline for managing cyber risk across rail's complex operational, safety and interface environments.

A key finding of this report is that the challenge is not simply the existence of cyber security risk, but the absence of a consistent national approach for managing that risk in a rail-specific context. Australia's vertically separated rail model means cyber risk is often shared across operators, infrastructure managers, suppliers, maintainers and project delivery bodies. This creates uncertainty around accountability, assurance and minimum acceptable security requirements, particularly where rolling stock and systems interact across jurisdictional boundaries.

AS 7770 provides an appropriate starting point because it is already tailored to the Australian rail industry and recognises the importance of cyber security governance in maintaining safe and reliable rail operations. However, the report has also identified that AS 7770, in its current form, is too high-level to function effectively as a mandatory or nationally harmonised standard without further uplift. Its principles-based structure provides flexibility, but does not provide enough prescriptive, assessable or auditable requirements to ensure consistent implementation across the sector.

The comparison with IEC 62443 highlights the value of more detailed operational technology cyber security requirements, particularly in relation to zones and conduits, lifecycle assurance, supplier obligations, technical security levels and evidence-based conformance. However, IEC 62443 alone is not sufficient for the Australian rail environment because it is not rail-specific and does not fully address the interoperability, safety assurance and shared accountability challenges created by Australia's rail operating model. This supports the case for an uplifted AS 7770 that draws on international best practice while remaining grounded in Australian rail conditions.

The report therefore justifies a hybrid approach: modernising AS 7770 into a stronger rail-specific umbrella standard, aligned with IEC 62443 and capable of future alignment with IEC 63452. This would allow Australia to establish a consistent national baseline for rail cyber security while still applying requirements proportionately across different types of operators, infrastructure, technologies and maturity levels.

This approach is justified because it balances consistency with practicality. A single rigid standard could create cost and capability barriers, particularly for smaller, regional or legacy networks. However, continuing with fragmented voluntary arrangements risks inconsistent cyber maturity, duplicated assurance effort and weakened trust at network interfaces. A tiered, risk-based implementation model would allow the industry to establish minimum cyber security expectations for interoperability while providing a structured pathway for progressive maturity uplift.

Overall, this report concludes that a nationally harmonised and uplifted AS 7770 is both necessary and achievable. It would strengthen cyber resilience, support Digital Train Control and ETCS implementation, improve supplier and project assurance, and better integrate cyber security into rail safety and governance frameworks. Most importantly, it would recognise cyber security as an essential enabler of safe, reliable and interoperable rail operations — not as a separate technical function, but as a core part of Australia's future rail safety and reform agenda.

10.0 REFERENCES

1. Rail Industry Safety and Standards Board. (2018). AS 7770:2018 Rail Cyber Security

2. Standards Australia. (2024). AS IEC 62443.3.2:2024 – Security risk assessment for system design: Standards Australia.

3. Standards Australia. (2024). AS IEC 62443.3.3:2024 – System security requirements and security levels : Standards Australia.

4. Standards Australia. (2025). AS IEC 62443.2.1:2025 – Security program requirements for IACS asset owners: Standards Australia.

5. Standards Australia. (2024). AS IEC 62443.4.1:2024 – Secure product development lifecycle requirements: Standards Australia.

6. Standards Australia. (2025). AS IEC 62443.4.2:2025 – Technical security requirements for IACS components: Standards Australia.

7. Standards Australia. (2024). AS IEC 62443.2.4:2024 – Security program requirements for IACS service providers: Standards Australia.

8. Queensland Government 2026, Information and cyber security policy (IS18), Queensland Government https://www.forgov.qld.gov.au/information-technology/queensland-government-enterprise-architecture-qgea/qgea-directions-and-guidance/qgea-policies-standards-and-guidelines/information-security-policy-is18

9. Standards Australia. (2025). Standards Australia adopts world's most foremost standard for operational technology, Standards Australia https://www.standards.org.au/news/standards-australia-adopts-worlds-foremost-standard-for-operational-technology

10. Kambourian. (2026). IEC 63452 – railway sector cyber security standardisation and Australian relevance, Anchoram Consulting https://anchoramconsulting.com/au/blog/security/iec-63452-railway-sector-cyber-security/

11. Australian Signals Directorate (ASD) 2025, Annual Cyber Threat Report 2024–25: Critical Infrastructure Factsheet, Australian Cyber Security Centre, Canberra https://www.cyber.gov.au/sites/default/files/2025-10/Annual%20Cyber%20Threat%20Report%202024-25%20factsheet%20for%20critical%20infrastructure.pdf

12. Grand View Research 2026, Australia Railway Cybersecurity Market Size & Outlook, 2033, Grand View Research, San Francisco https://www.grandviewresearch.com/horizon/outlook/railway-cybersecurity-market/australia

13. ITMM Communique, 11 August 2025. https://www.infrastructure.gov.au/sites/default/files/documents/itmm-communique-11-august-2025.pdf