RISSB

RAIL INDUSTRY SAFETY AND STANDARDS BOARD

Rail Cyber Security

(Implementation of AS 7770:2018)

Guideline

This Rail Industry Safety and Standards Board (RISSB) product has been developed using input from rail experts from across the Rail Industry. RISSB wishes to acknowledge the positive contribution of all subject matter experts and DG representatives who participated in the development of this product.

The RISSB Development Group for this guideline consisted of representatives from the following organisations:

Abbott Risk Consulting	Aurizon	Australian Cyber Security Centre
BHP Billiton	Bombardier	Downer Group
Envista	KiwiRail	Metro Sydney
Metro Trains Melbourne	Pacific National	Rail Assurance Consulting
Rail Control Systems Australia	Rail Systems Australia	Roy Hill
Sydney Trains	Tobruk Security	V/Line
VicTrack		

Development of this guideline was undertaken in accordance with RISSB's accredited processes. It was approved by the Development Group, endorsed by the Standing Committee, and approved for publication by the RISSB Board.

I commend this guideline to the Australasian rail industry as part of the suite of RISSB products assisting the rail industry to manage rail safety, improve efficiency and achieve safety outcomes through interoperability and harmonisation.

Deb Spring
Exec. Chair / CEO
Rail Industry Safety and Standards Board

Notice to users

The reliance upon or manner of use of this RISSB product is the sole responsibility of the user who is to assess whether it meets their organisation's operational environment and risk profile.

RISSB
RAIL INDUSTRY SAFETY AND STANDARDS BOARD

Keeping guidelines up to date

To maintain their currency, guidelines developed by RISSB are periodically reviewed, and new editions published when required. Between editions, amendments can be issued.

It is important that readers assure themselves of that they are using a current RISSB guideline. Information about RISSB guidelines, including amendments, can be found by visiting www.rissb.com.au.

RISSB welcomes suggestions for improvements and asks readers to notify us immediately of any apparent inaccuracies or ambiguities, please contact us via email at info@rissb.com.au or write to Rail Industry Safety and Standards Board, PO Box 518, Spring Hill, QLD 4004, Australia.

RISSB product can be found at: http://www.rissb.com.au/products/.

Document control

Identification

Document Title	Version	Date
Rail Cyber Security (Implementation of AS 7770:2018) Guideline	1.0	21 June 2019

Document history

Publication Version	Effective date	Page(s) Affected	Reason for and extent of changes
1.0	21 June 2019	All	First published

Approval

Name	Date
Rail Industry Safety and Standards Board	21 June 2019

Copyright

Contents

1 Introduction

Advanced malicious cyber activity against Australia's national and economic interests is increasing in frequency, scale, sophistication and severity. The reach and diversity of cyber adversaries are expanding, and their operations against both government and private networks are constantly evolving[1].

The effective management of cyber security risk and the controls used to mitigate that risk to acceptable levels is likewise increasing in its strategic importance for all organisations.

Standards and practices used to manage cyber security risk have evolved primarily in government, defence and information technology intensive industries. Now generally adopted in all industries, typically within the remit of corporate IT functions, the focus has been and remains on the protection of information and critical business processes.

Within organisations more heavily dependent on operational technology (OT) cyber security risk management has been historically confined to the IT domains of their operations with OT being more generally protected from these risks by physical separation of networks, the highly specialised nature of many OT systems and mature practices applied within engineering lifecycles.

However, the increasing complexity and interconnectedness of rail management and control systems and the increasing use of commercial-off-the-shelf (COTS) products mean that OT systems are now more vulnerable to the same cyber security risks that were previously confined to the domain of IT.

This creates the alarming possibility that attacks occurring in the cyber domain could have an impact on critical infrastructure and human safety.

In response to this convergence of safety risk, business risk, and cyber security risk, the Rail Industry Safety and Standards Board (RISSB) facilitated the development of The Australian Standard AS 7770:2018 – Rail Cyber Security ("The Standard") and this accompanying implementation guideline.

The Standard brings together the safety focus of the rail industry with the approaches of cyber security used more generally in corporate IT so that cyber security risks now relevant in the increasingly "connected" operational domains and investment programmes of the rail industry can be more effectively managed.

1.1 Purpose

The Australian Standard AS 7770:2018 – Rail Cyber Security ("The Standard") specifies the requirements for Rail Transport Operators (RTOs) for managing cyber security risk on the Australian Railway Network.

This guideline accompanies the Standard and provides implementation guidance for organisations seeking to implement (or needing to comply with) the requirements of the Standard.

This guideline needs to be read in conjunction with the Standard.

[1] Australian Cyber Security Centre "ACSC Threat Report 2017"

1.2 Intended Audience

The Standard applies primarily to rail transport operators (RTOs), industry suppliers, subcontractors and maintenance contractors who are operating in an industry which is facing new and emergent risks of cyber security attack on critical infrastructure and have changed expectations from industry participants for the effective management of cyber security risks.

This guideline has been authored to address a primary audience of engineering and technology managers in these organisations. It is assumed that they have a general understanding of cyber security principles, rail safety, and control systems.

Secondary audiences for this guideline include personnel working in these organisations with interests in governance, leadership, strategy, safety, risk management, programme management, technology and compliance.

1.3 Documents and Content

The documents comprising the suite of AS 7770:2018 include the following:

- AS 7770:2018 - Rail Cyber Security ('The Standard').
  Each section of the standard provides:
  - background and intent;
  - mandatory requirements;
  - recommended requirements.
- Rail Cyber Security Guideline (Implementation of AS 7770:2018) ('This Document').
  The major sections of this guideline include the following:
  - Introduction:
    - Introductory comments, key points on application and compliance, and definitions.
  - Implementation approaches:
    - Guidance and examples of the approaches that organisations take for setting business relevant cyber security goals; developing a cyber security strategy; setting up the fundamentals; and implementing cyber security initiatives using a combination of iterative and programmatic approaches.
  - Specific guidance aligning to the three major sections of the Standard:
    - Rail Transport and Cyber Security Risk Management.
    - Principles of Effective Cyber Security Design.
    - Managing Cyber Security Effectively.
- Codes of Practice published in relation to AS 7770:2018:
  - Code of Practice - Rail Cyber Security in Rolling Stock.
  - Code of Practice – Rail Cyber Security in Train Control Systems.

1.4 Application and Compliance

This guideline explores topics of implementation. It does not form part of the Standard itself. Users of the Standard and this guideline should note: