RISSB
RAIL INDUSTRY SAFETY AND STANDARDS BOARD

Security Handbook for Small to Medium Rail Transport Operators

Volume 2

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:

Aurecon Group
Department of Transport Victoria
Jacobs Group (Australia) P/L
KiwiRail
Marling Group
Transport for NSW
VLine Corporation

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 Standard to the Australasian rail industry as it represents industry good practice and has been developed through a rigorous process.

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

Notice to users

This RISSB product has been developed using input from rail experts from across the rail industry and represents good practice for the industry. 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.

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

Document title	Version	Date
Security Handbook for Small to Medium Rail Transport Operators - Volume 2	2020	23 June 2020

Document history

Publication version	Date	Reason for and extent of changes
2009 Edition	May 2009	Approved for issue by RISSB Board and ARA Executive
2020 Edition	23 June 2020	Revised Edition - Approved for issue by RISSB Board

Approval

Name	Date
Rail Industry Safety and Standards Board	23/06/2020

Copyright

References

Legislation	
Rail Safety National Law (South Australia) Act 2012	Rail Safety National Law National Regulations 2012
Rail Safety National Law (NSW) No 8a	Rail Safety (National Uniform Legislation) Act 2012 No 27 (NT)
Rail Safety (National Uniform Legislation) Regulations 2015 (NT)	Rail Safety National Law (Tasmania) Act 2012 No 38
Rail Safety National Law Application Act 2013 No 22 (VIC)	Rail Safety National Law (ACT) Act 2014
Rail Safety National Law (WA) Act 2015	Rail Safety National Law (WA) Regulations 2015
Rail Safety National Law (Queensland) Act 2017	Rail Safety National Law (Queensland) Regulation 2017
Commonwealth Places (Application Of Laws) Act 1970 (Commonwealth)	Control of Weapons Act 1990 (Vic)
Control of Weapons Regulations 2000 (Vic)	Criminal Code Act 1995 (Commonwealth)
Drugs, Poisons and Controlled Substances Act 1981 (Vic)	Environmental Planning and Assessment Amendment (Infrastructure and Other Planning Reform) Act 2005 (NSW)
Evidence Act 2008 (1958) (Vic)	Firearms Act 1996 (Vic)
Health and Safety in Employment Act 1992 (NZ)	Information Act 2002 (NT)
Information Privacy and Data Protection Act 2014 (Vic)	Information Privacy Act 2000 (Vic)
Injury Prevention, Rehabilitation, and Compensation Act 2001 (NZ)	Intelligence Services Act 2001 (Commonwealth)
Justice Legislation Amendment (Terrorism) Act 2019 (NSW)	Major Events (Crowd Management) Act 2004
Maritime Transport and Offshore Facilities Security Act 2003 (Commonwealth)	Occupational Health and Safety (Commonwealth Employment) Act 1991 (Commonwealth)
National Security Information Act (2004) Commonwealth	Work Health and Safety Act 2011 (ACT)
Workplace Health and Safety Act 2011 (NSW)	Occupational Health and Safety Act 2004 (Vic)
Work Health and Safety Law 2012 (SA)	Occupational Safety and Health Act 1984 (WA)
Privacy Act 1988 (Commonwealth)	Privacy and Data Protection Act 2014 (Vic)
Privacy and Personal Information Protection Act 1998 (NSW)	Private Investigators and Security Guards Act 1974 (NZ)
Private Security Act (NT)	Private Security Act 2004 (Vic)
Public Records Act 2002 (Qld)	Rail Safety Act 1996 (SA)
Rail Safety Act 1997 (Tas)	Rail Safety Act 1998 (WA)
Rail Safety Act 2006 & Rail Safety Regulations2006 (Vic)	Railway Safety and Corridor Management Act 1992 (NZ)
Right to Information Act 2009 (Tas)	Security and Investigation Agents Act 1995 (SA)
Security and Investigations Agents Act 2002 (Tas)	Security and Related Activities (Control) Act 1996 (WA)
Security Industry Act 1997 (NSW) & Security Industry Amendment Act 2005 (NSW)	Security Industry Act 2003 (ACT)
Security Legislation Amendment (Terrorism) Act 2002 (Commonwealth)	Security of Critical Infrastructure Act 2019 (Commonwealth)
Security Providers Act 1993 (Qld)	Surveillance Devices Act (Workplace Privacy) Act 20061999 (Vic)
Surveillance Devices Act 1999 (Vic)	Terrorism (Commonwealth Powers) Act 2002 (NSW)
Terrorism (Commonwealth Powers) Act 2002 (Qld)	Terrorism (Commonwealth Powers) Act 2002 (SA)
Terrorism (Commonwealth Powers) Act 2002 (Tas)	Terrorism (Commonwealth Powers) Act 2002 (WA)
Terrorism (Commonwealth Powers) Act 2003 (Vic)	Terrorism (Community Protection) Act 2003 (Vic)
Terrorism (Community Protection) Amendment 2018 (Vic)	Terrorism (Emergency Powers) Act 2003 (NT)
Terrorism (Police Powers) Act 2002 (NSW)	Work Health Act (NT)
Workplace Health and Safety Act 2011 (Qld)	Workplace Health and Safety Act 2012 (Tas)
Workplace Surveillance Act 2005 (NSW)	Workplace Video Surveillance Act 1998 (NSW)

Standards	
AS/NZS 2201.1: 2007 Intruder alarm systems – Systems installed in client's premises	AS 2201.5:2008 Intruder alarm systems – Alarm transmission systems
AS 3555.1: Building Elements – Testing and rating for intruder resistance – Intruder-resistant panels	AS 3745:2010 Emergency control organisation and procedures for buildings, structures and workplaces
AS 4145.1:2008 - Locksets – Glossary of terms	AS 4485 Set:1997 – Security for health care facilities
AS 4145.2:2008 - Locksets – Mechanical locksets for doors in buildings	AS 4806:2008 Set
AS 4811: 2006 - Employment Screening	AS 5039:2003 – Security screen doors and security window grills
AS 5040:2003 – Installation of security screen doors and windows	AS 5041:2003 – Methods of test – Security screen doors and window grills
AS 7770 – Rail Cyber Security	AS 8000:2003 - Corporate Governance – Good governance principles
AS/ISO 27799:2011 - Information security management in health using ISO/IEC 27002	AS/ISO/IEC 27001 and 27002 IT Security Set: 2015 – Information technology - Security techniques
AS/ISO/IEC 27013:2017- Information technology - Security techniques - Guidance on the integrated implementation of ISO/IEC 27001 and ISO/IEC 20000-1	AS ISO/IEC 27035 Set2017- Information technology - Security techniques - Information security incident management
AS/ISO/IEC 27002:2015- Information technology - Security techniques - Code of practice for information security controls	AS/NSZ ISO/IEC 11770 Security Set: 2008 – Information technology – Security techniques – Key management
AS/NZS 1170.2:1170.2:2002 – Structural Design Actions – Part 2: Wind Actions	AS/NZS IS O/IEC 9798 Set:2008- Security for health care facilities - General requirements Information technology - Security techniques
AS/NZS ISO/IEC 17799:2005 Information technology – Code of practice for information security management	AS/NZS ISO/IEC 17799:2006 - Information technology - Security techniques - Code of practice for information security management
AS/NZS ISO/IEC 18028:2008 - Information technology - Security techniques - IT network security - Network security management	AS/NZS ISO/IEC 27005:2012 – Information technology - Security techniques - Information security risk management (ISO/IEC 27005:2011, MOD)
AS/NZS ISO/IEC 27011:2017 – Information technology - Security techniques - Code of practice for information security controls based on ISO/IEC 27002 for telecommunications organizations	AS/NZS ISO/IEC:2005 – Information technology – Security techniques – information security management systems - Requirements
HB 158 – Delivering assurance based on AS/NZS ISO 31001	HB 167:2006 - Security risk management
HB 171:2003 – Guidelines for the management of IT evidence	HB 231:2004 - Information security risk management
HB 240 Guidelines for managing risk in outsourcing	HB 324:2008 - Lexicon of key terms used in security
HB 327 – Communicating and Consulting about Risk	HB 328:2009 - Mailroom security
HB 436 – Risk Management Guidelines – Companion to AS/NZS ISO 31001	ISO 31000:2018: Risk management Guidelines
ISO Guide 73 – Risk Management – Vocabulary	Protective Security Policy Framework (Commonwealth)
SRMBOK RMIA 2008	Victorian Protective Data Security Standard (VPDSS)

Other	
A National Approach to Closed Circuit Television – National Code of Practice for CCTV Systems for the Mass Passenger Transport Sector for Counter Terrorism (COAG July 2006)	ANZCTC – National Guidelines for Protecting Critical Infrastructure from Terrorism 2015
ANZCTC – Hostile Vehicles Guidelines for Crowded Places 2017	ANZCTC – National Counter-Terrorism Plan 2017
ANZCTC – Australia's Strategy for Protecting Crowded Places from Terrorism 2017	ANZCTC – Active Offender Guidelines for Crowded Places 2017
ANZCTC – Improvised Explosives Devices (IED) Guidelines for Crowded Places 2017	ANZCTC – Chemical Weapon Guidelines for Crowded Places 2017
ASIO Mass Passenger Transport Systems Risk Context Statement June 2014	Attorney-General's Department (2005) National Counter-Terrorism Plan, Canberra: CoA
Attorney General's Department (2017) National Counter-Terrorism Plan	Attorney General's Department - Protective Security Policy Framework (Critical Infrastructure Protection)
Attorney General's Department Critical Infrastructure Resilience Strategy Plan 2015	Attorney-General's Department – Managing the Insider Threat to your business – A personnel security handbook
Attorney-General's Department - Physical Security Management Protocol 2011	Australian Government – COMCOVER – Better Practice Guide – Risk Management 2008
Australian Government- Cyber Security Strategy 2009	Australian Government - Improvised Explosive Device (IED) Guidelines For Places Of Mass Gathering

Other	
Australian Government - Investigation Standards (AGIS) 2012	Australian Government – Organisational resilience – Critical Infrastructure 2011
Australian Government – Physical security Management Guidelines – Physical Security of ASIS International – ASIS ORM.1-2017 – Security and Resilience in Organizations and their Supply Chain – Requirements with Guidance	Australia's Counter Terrorism Strategy 2015
Building Code of Australia	Centre for the Protection of National Infrastructure – Security Lighting: Guidance for Security Managers 2015
Queensland Police Service - Crime Prevention Through Environmental Design (CPTED) Guideline (Parts A and B)	Commonwealth Attorney-General's Department (2005) Commonwealth Protective Security Manual, Canberra: CoA
CPNI UK – Door Security 2013	CPNI UK – CCTV for CNI Perimeter Security 2014
CPNI UK – Integrated Security Guide for Hostile Vehicle Mitigation 2nd Edition 2014	CPNI UK – Integrated Security Guide for Hostile Vehicle Mitigation 2nd Edition 2014
CPNI UK - Levels 1 and 2 Operational requirements for Hostile Vehicle Mitigation 2010	CPNI UK – Protecting against Terrorism 3rd Edition 2010
Crowded-places-security-audit	Dept of Home Affairs – National Surface Transport Security Strategy
Dept of Home Affairs – National Code of Practice for CCTV Systems for mass passenger transport sector for counter-terrorism	Department of Infrastructure - National Policy Framework for Land Transport Technology
Department of Transport CPNI (SIDOS) UK – Security in Design of Stations 2012	Dr Miles Jakeman – Citadel Group Limited - Australia – Guide to SRMBOK RMIA – Physical Security Specifications and Postures
Handling and Transporting Cash – Security Risks – General Guide 2014	HM Government UK – Protecting Crowded Places – Design and Technical Issues 2014
Home Office Scientific Development Branch UK – CCTV Operational Requirements Manual 2009	ICT equipment, systems and facilities 2011
Information Privacy Principles Instruction (SA)	Inter-Governmental Agreement for Surface Transport Security
International Union of Railways – Station Security for Station Business	National Critical Infrastructure Resilience Strategy July 2016
National Guidelines For The Protection Of Places Of Mass Gathering From Terrorism September 2010	National Guidelines for Protecting Critical Infrastructure from Terrorism Protecting Crowded Places from Terrorism 2017
Risk Management Institute of Australia (RMIA) – Security Risk Management Body of Knowledge	RISSB Security Handbook Vol 1 - Managing Security Related Risks in Rail Organisations
RISSB Code of Practice – Rail Cyber Security in Rollingstock	RISSB Code of Practice – Rail Cyber Security in Train Control
RISSB Guideline – Implementation of AS 7770	State Government of Victoria – Guide to Develop CCTV for Public Safety in Victoria
Transport and Infrastructure Senior Official Committee, A national approach to close circuit television, national code of practice for CCTV systems for the mass passenger transport for counter-terrorism	Trusted Information Sharing Network for Critical Infrastructure Protection – Defence in Depth 2008
USA MTI – The Challenge of Protecting Transit and Passenger Rail – Understanding how Security works against Terrorism	US Department of Transport – Transit Security Design Considerations 2004
UFC 4-022.02 – Selection and Application of Vehicle Barriers 2009	UFC 4-010-01 – DoD Minimum Antiterrorism Standards for Buildings
Victorian Critical Infrastructure Resilience Strategy July 2016	Victorian Ministerial Guidelines for Critical Infrastructure Resilience

Hazard table

Hazard Number	Hazard	Section addressing
3.2	A breach of security	All sections
3.3	Harm to an organisation	All sections

Contents

Annexes

1 Overview

1.1 Introduction

This document has been prepared as a guide for conducting a security risk assessment for small to medium rail transport operators (RTOs). The approach taken in the handbook recognises that, RTOs are best placed to determine the vulnerabilities and threats to their assets (being their people, property, information, operations, reputation and environment), as well as identifying appropriate preventative security measures and/or procedures and to develop appropriate security risk management plans (SRMP).

This handbook has been developed to expand on information available in Security Handbook Vol 1 Managing Security Related Risks in RTOs. In addition to providing a systematic process, it also explains how that process fits with the overall management of security in an RTO and provides direction on how to make use of the process outcomes to demonstrate the management of risk to So Far As Is Reasonably Practicable (SFAIRP)

The example framework (RAILRISK) aims to provide a means of identifying and managing those things that could happen (i.e. the risks), and that might impact on the achievements of a RTO's objectives, from a security perspective. RAILRISK is applicable to all activities, elements, and functions at all levels across the RTO and output from RAILRISK will be used to produce a SRMP for small to medium RTOs.

It is not viable for protective security measures to be applied as a matter of course – they need to be commensurate with the level of risk applicable to the asset, resource, or function to be protected. RAILRISK evaluates risk levels and the consequent allocation of resources to ensure that protective security measures accord with the determined levels of risk.

RTOs should ensure that the security risk assessments take into account the legislative and any other requirements. RTOs should utilise the ISO 31000 standard, the HB:436:2004 Risk Management Handbook, and the HB 167:2006 Security Risk Management Handbook, or an equivalent risk management standard as defined in their safety management system (SMS), together with this handbook when completing their security risk assessments.

1.2 Purpose

RAILRISK provides a framework based on the widely accepted risk management process from ISO 31000, to enable RTOs to demonstrate that the identified risks have been adequately analysed and evaluated, and that appropriate preventative security strategies have been identified to treat those identified risks to SFAIRP

This document will extend the risk management process to provide additional detail in respect of the following:

- The application of mandatory minimum standards (legislation and regulations).
- Comparative benefit analysis of risk treatment options, including potential impost on resources.
- The development of action plans to ensure that selected treatment options are implemented and monitored.
- A formal mechanism for sharing responsibility for a security risk that cannot be managed effectively by the risk owner.