AS 7770:2018

Australian STANDARD®

# Rail Cyber Security

RISSB
RAIL INDUSTRY SAFETY AND STANDARDS BOARD

Safety Standard

This Australian Standard® AS 7770 Rail Cyber Security was prepared by a Rail Industry Safety and Standards Board (RISSB) Development Group consisting of representatives from the following organisations:

Click here to enter the organisations represented on the Development Group. Tab between them.

The Standard was approved by the Development Group and the Enter Standing Committee Standing Committee in Select SC approval date. On Select Board approval date the RISSB Board approved the Standard for release.

Choose the type of review

Development of the Standard was undertaken in accordance with RISSB's accredited process. As part of the approval process, the Standing Committee verified that proper process was followed in developing the Standard.

RISSB wishes to acknowledge the positive contribution of subject matter experts in the development of this Standard. Their efforts ranged from membership of the Development Group through to individuals providing comment on a draft of the Standard during the open review.

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

**Paul Daly**
Chief Executive Officer
Rail Industry Safety and Standards Board

## Keeping Standards up-to-date

Australian Standards developed by RISSB are living documents that reflect progress in science, technology and systems. To maintain their currency, Australian Standards developed by RISSB are periodically reviewed, and new editions published when required. Between editions, amendments may be issued. Australian Standards developed by RISSB may also be withdrawn.

It is important that readers assure themselves they are using a current Australian Standard developed by RISSB, which should include any amendments that may have been issued since the Standard was published. Information about Australian Standards developed by RISSB, 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. Members are encouraged to use the change request feature of the RISSB website at: http://www.rissb.com.au/products/. Otherwise, please contact us via email at info@rissb.com.au or write to Rail Industry Safety and Standards Board, PO Box 4271, Kingston ACT 2604, Australia.

# AS 7770:2018

**Rail Cyber Security**

## Document details

First published as: Enter first publication identifier (AS XXXX:yyyy)

ISBN Enter ISBN.

Published by SAI Global Limited under licence from the Rail Industry Safety and Standards Board,
PO Box 4271, Kingston ACT 2604, Australia

## Copyright



## 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.

# Document control

## Document identification

| Designation / Title |
|---|
| AS 7770:2018 Rail Cyber Security |

## Document history

| Publication Version | Effective Date | Reason for and Extent of Change(s) |
|---|---|---|
| 2018 | Select Board approval date | |
| | | |
| | | |

## Draft history

| Version | Date | Change(s) |
|---|---|---|
| 1.0 | 27 June 17 | Draft of TOC and Hazards |
| 1.1 | 14 August 17 | Draft Content of Standard |
| 1.2 | 17 September 17 | For review by Development Group |
| 1.3 | 20 October 17 | Amendments prior to public comment |
| 2.0 | 30 October 2017 | Draft for public consultation |

## Approval

| Name | Date |
|---|---|
| Rail Industry Safety and Standards Board | Select Board approval date |

# Contents

## Appendix Contents

# 1 Introduction

## 1.1 Purpose

This Standard specifies the requirements for Rail Transport Operators (RTOs) for managing cyber security risk on the Australian Railway Network.

It has been developed to assist RTOs to establish and maintain a good practice approach to Operational Technology (OT) and Information Technology (IT) that is used within their organisations to operate rail systems, and protect them from deliberate cyber-attack.

## 1.2 Scope

The scope of this Standard is to cover the elements of OT/IT that are at risk to cyber breaches or attacks impacting on the safe operation of the railway network.

This Standard includes the requirements for:

- Determining the scope of cyber security as it effects safety.
- Protecting rail infrastructure and rolling-stock systems.
- Train Control Systems protection.
- Risk assessment and management.
- Principles for effective cyber security.
- Concepts for effective cyber security.
- Designing in security.
- Design.
- Protecting against attacks on new and current systems.
- General guidance applicable to all systems.
- Competence and compliance.
- Customer and passenger control.
- Handling threats and incidents.
- A rise in threat level or unexpected attack.
- Contingency in the event of a cyber attack.
- Clear up and recovery.

## 1.3 Intended Audience

This guidance applies primarily to RTOs and applicable to suppliers, subcontractors and maintenance contractors, who will need to be aware of changing expectations in the industry that they are supporting.

This Standard has been written for use by digital systems engineers or security architects who have a detailed knowledge of rail control systems, critical systems design and cyber security. It is assumed that the reader is familiar with the information security body of knowledge required for certifications such as the CISSP (ISC2) or CISM (ISACA).

To implement this Standard, the reader is considered to be proficient in security architecture methodologies (e.g. SABSA) and familiar with the normative references in this Standard.

This Standard is not specifically intended to cover urban on-street tramway, light rail networks, or heritage railways operating on a private reservation, but may be applied to such systems as deemed appropriate by the relevant organisation.

## 1.4 Compliance

There are two types of control contained within Australian Standards developed by RISSB:

a) Mandatory requirements; and

b) Recommended requirements.

Each of these types of control address hazards that are deemed to require controls based on existing Australian and international Codes of Practice and Standards.

A mandatory requirement is a requirement that the Standard provides as the only way of treating the hazard.

***Mandatory*** requirements are identified within the text by the term 'shall'.

A recommended requirement is one where the standard recognises that there are limitations to the universal application of the requirement and that there may be circumstances where the control cannot be applied or that other controls can be appropriate or satisfactory, subject to agreement with the Rail Infrastructure Manager (RIM), Rolling Stock Operator (RSO), and/or Rail Safety Regulator.

***Recommended clauses*** are mandatory unless the RIM or RSO can demonstrate a better method of controlling the risk.

Recommended requirements are identified within the text by the term 'should'.

Hazards addressed by this Standard are included in an appendix.

Refer to the RISSB website for the latest Hazard Register Guideline.

## 1.5 Referenced documents

### 1.5.1 Normative references

The following referenced documents are indispensable for the application of this Standard:

a) ISO/IEC 27000 series;

b) NIST Cybersecurity Framework;

c) NIST SP800-30 Revision 1 Guide for Conducting Risk Assessments, NIST;

d) NIST SP800-82 Revision 2 Guide to Industrial Control Systems (ICS) Security, NIST.

### 1.5.2 Informative references

The following referenced documents are used by this Standard for information only:

a) ANSI/ISA-62443-2-1 (99.02.01)-2009 - Security for Industrial Automation and Control Systems: Establishing an Industrial Automation and Control Systems Security Program;

b) BS EN 50159:2010 - Railway applications. Communication, signalling and processing systems. Safety-related communication in transmission systems, British Standards International, 2010;

c) ISO/IEC TR 15443-1:2012 Information technology -- Security techniques -- Security assurance framework -- Part 1: Introduction and concepts, ISO;

d) ISO/IEC TR 15443-2:2012 Information technology -- Security techniques -- Security assurance framework -- Part 2: Analysis, ISO;

e) The CIS Critical Security Controls for Effective Cyber Defense, SANS;

f) Cobit 5 for Information Security, ISACA;

g) Cyber security Procurement Language for Control Systems, US Department of Homeland Security;

h) Cybersécurité des systèmes industriels : Mesures détaillées (tr. Cyber security for Industrial Control Systems : detailed measures), ANSSI;

i) Cyber security Informed Safety Cases for the Rail Industry: Code of Practice, Department for Transport Rail Executive (UK);

j) Essential 8 Cyber security Strategies, Australian Signals Directorate;

k) Industrial Internet of Things Volume G4: Security Framework, Industrial Internet Consortium;

l) OCTAVE Method;

m) Rail Cyber security Guidance to Industry, Department of Transport (UK);

n) Rail Cyber security, Release 1.1, January 2017, Rail Delivery Group

o) Recommended Practice: Improving Industrial Control System Cyber security with Defense-in-Depth Strategies, US Department of Homeland Security;

p) Saltzer, Jerome H., and Michael D. Schroeder. "The protection of information in computer systems." Proceedings of the IEEE 63.9 (1975): 1278-1308;

q) SB 800-53 rev 4, Security and Privacy Controls for Federal Information Systems and Organizations, NIST.

## 1.6 Definitions

***Ancillary System:*** Any computer application, device or networks used in the delivery of rail services by rail transport operators which are not classified as rail control systems. This can include ticketing systems (including payment systems), security monitoring, and access control systems.

***Corporate Systems:*** Computer applications, device and networks that are used to support the corporate functions of a rail transport operators, which do not have an immediate and direct impact on the safe and reliable operation of railways. Examples could include staff rostering, payroll and human resource systems, ERP systems, and corporate desktop applications such as work processing.

***Cyber Attack***: Attempt to destroy, expose, alter, disable, steal or gain unauthorised access to or make unauthorised use of a rail control system or ancillary system used in the operation of railways.

***Cyber Security Incident:*** An unwanted or unexpected cyber security event that has a significant probability of compromising business or railway operations. It may threaten a breach of confidentiality, integrity, or availability of digital assets. May be directly caused by a cyber attack or security breach, or be related to cyber security by other events that result in a cyber security incident(s).

***Cyber Security Risk:*** A function of the likelihood of a given threat exercising a potential vulnerability, and the resulting impact of that adverse event on the organisation.

***Cyber Threat:*** The malicious action that can be exercised in and throughout cyberspace, or against it and its fundamental elements. These may be immediate or develop overtime.

***Control Objective:*** Statement describing what is to be achieved as a result of implementing controls.

***Information Technology (IT)***: Application of computers to store, retrieve, transmit and manipulate data in the context of a business or other enterprise.

***Operational Technology (OT):*** Systems which are directly responsible for the functioning of the operational railway, including railway network infrastructure and rolling-stock.

***Rail Cyber Security:*** Preservation of availability, integrity and confidentiality of information and the Reliability, Availability, Maintainability and Safety (RAMS) of Rail control systems.

***Rail Control System***: Any system (application, device or network) that controls the operation of trains or railways. This includes all forms of signalling and switching, locomotive or train operation (either autonomous or via operator), train communications system, passenger management, power reticulation, or level crossings.

***Rail Transport Operator*** **(RTO):** An organisation that has an agreement with a Rail Infrastructure Manager to enter and use a rail Network. Means- A rail infrastructure manager or rolling stock operator or a person who is both a rail infrastructure manager and a rolling stock operator.

***Threat Source:*** The intent and method targeted at the intentional exploitation of a vulnerability or a situation and method that may accidentally exploit a vulnerability.

***Threat Actions:*** The action that a threat source may carry out to attack a system.

***Vulnerability:*** A weaknesses in systems, system procedure(s), information systems, security measures, or implementations, that can be exploited by a threat source to cause a cyber security event or incident. Vulnerabilities can arise from many sources, including: policy and procedures, architecture and design, configuration and maintenance, physical intrusion, system software and product development, communication and networks, lack of training and awareness.

# 2 Rail Transport and Cyber Security Risk

## 2.1 Rail Transport Introduction

### 2.1.1 Digital Technology

Technology is critical to the railway, supporting business and operational needs. Broadly, computer- based railway systems can be divided into two environments that have varying cyber security risks, business drivers and potential impacts of loss or failure:

- Business systems that deliver corporate or enterprise functions, and include systems that support and provide interface to the operational railway.
- Operational systems that enable the operational railway to function through control of network infrastructure and rolling stock.

Technology is enhancing efficiency and customer service across the railway. This means that the two environments are converging so that:

- Information is increasingly exchanged between business systems, operational systems and organisations to support railway performance and safe interworking, and

- The industry is increasingly reliant on computer- based technology, now common to both environments, which has security implications.

Organisational and system interfaces, as well as the workforce using the technology, also increase the exposure of the railway. Additionally, a large and widely dispersed volume of railway assets, which can be difficult to protect, could provide access points for cyber threats.

### 2.1.2 Rail Cyber Security Risk

Rail cyber-attack has the potential to result in any of the following outcomes:

- Threats to safety-
- Disruption to network operations-
- Economic loss to operators, suppliers and the wider Australian community-
- Reputational damage to rail organisations and government-
- Loss of commercial and sensitive information-
- Criminal damage.

## 2.2 The Threat

### 2.2.1 Intent

The intent of this section is to emphasise the importance of embedding threat assessment as part of the systematic management of security risk in rail systems.

### 2.2.2 Requirements

The RTO:

a) shall develop and document an understanding of their cyber security threat context, which includes identifying threat sources, systems architectures of systems, organisational structures and interfaces relevant to cyber security, and legal and regulatory requirements.

b) shall communicate the cyber security threat context to their senior managers and board members and ensure they are informed about cyber security risk.

c) should regularly (at least annually) review the threat context to detect and highlight any emerging trends that can change the risk context that the RTO operates in.

d) shall implement a systematic methodology for the identification and evaluation of cyber threats.

e) shall adopt a methodology that is based on a recognised threat assessment methodology.

f) shall not use the assessment of low likelihood of a threat to be the primary basis for acceptance of risk in a risk management plan, where the worst-case consequence is serious loss of safety or catastrophic loss of life.

### 2.2.3 Background and Rationale

#### 2.2.3.1 Threat Context

As RTOs enter the digital age, there is demand for control systems that are more sophisticated, functional, affordable, maintainable and able to more effectively share data in an inter-connected manner. Increasingly these systems are making more of the routine executive

decisions in train operations, possibly to the elimination of human decision making in the driving of trains. There are three major trends within rail systems that are important:

a) Increasing complexity in the requirements of rail management systems.
   - In the past control systems were required only to manage switching and signalling, today there are myriad of automated systems that collectively form the rail management system. This complexity and span of functions significantly increased the challenge of ensure secure operation.

b) The increasing interconnectedness of rail management systems with external networks.
   - Many in-service control systems were built on the assumption that cyber protection will be achieved by physical and electrical isolation. This is becoming an invalid assumption. The demand for more integration, better sharing of data and outsourcing of operations are all drivers to enable greater network connectivity. Logical access controls are increasingly replacing electrical isolation as the primary security mechanism on networks.

c) The trend of using more commodity commercial off-the-shelf (COTS) components and systems.
   - The complexity of systems, the requirement for extra functionality and the increasing drive to reduce design and operational cost is leading to the adopting of COTS components and sub-systems in the rail management system.

In this context, the rise of deliberate cyber-attack has become an issue that RTOs shall manage. Both internal and external actors should seek access to systems to cause damage that could range in their consequences from causing reputational damage, disruption of services, or even harm to people and equipment. Operation of controls such as Isolation of systems can be imperfect and it is probable that networks will at some point be compromised.

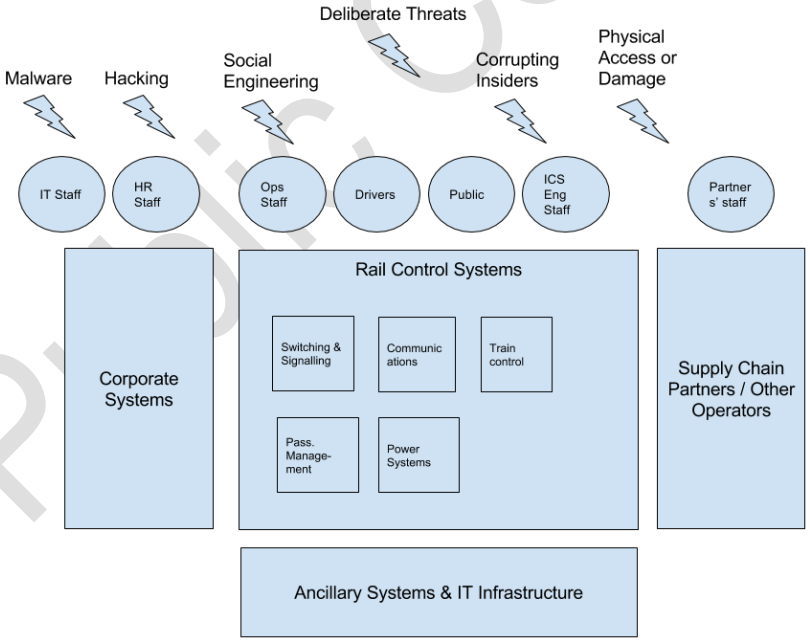


*Figure 1 - Rail Cyber Security Context*

#### 2.2.3.2 Threat Sources

Deliberate threat sources can be broken in the following categories:

a) Internal actors (staff, contractors and service providers)
   - Operational Staff
   - IT and OT Engineering Staff
   - Contractors and Service Providers
   - Supply-chain Partners
   - Other RTOs
   - Staff, not otherwise classified.

b) External actors
   - Cyber terrorists
   - Issue-motivated groups
   - Former staff and contractors
   - Cybercrime groups
   - Nation state actors
   - General Hackers.

Each of the categories have different motivations (financial, political, personal), capabilities (from using simple tools to development of novel malware) and freedom of action (are they willing to kill and injure people?).

#### 2.2.3.3 Threat Action

When a threat assessment is developed, it is important to consider likely and possible modes of action. The technical act of hacking will be a component of these threats. Often the actual group performing the technical breach can be commissioned by the primary threat i.e. a hackers-for-hire. This can be because of technical capability or to maintain a certain degree of deniability. It is common for the threat action to be a complex combination of actions. For example: a terror group could use a kinetic attack to disable control system while using hacking to identify vulnerable points to attack, to gain access to controlled areas, disable monitoring systems, or attack services required to run the railway such as power reticulation.

#### 2.2.3.4 Threat assessment

In assessing a threat, an organisation should assess the dimension of type, motivation, capability and freedom of action, remembering that efficient cyber defence needs to be built on an accurate assessment so that it is both efficient, economical and effective against most probable and most dangerous threat actions. Assessment of the likelihood of a threat manifesting is particularly challenging and differs from traditional assessment of environmental hazards as there can be little antecedent evidence to predict a threat and no current evidence of such a threat developing within a control system. For this reason, many threat assessments methodologies assume all threats are manifest and assess the impacts rather than likelihood.

There are several formal threat assessment methodologies that organisations can use to identify and assess threat. One example is the Octave methodology developed by CERT and the SEI.

## 2.3 Controls and Vulnerabilities

### 2.3.1 Intent

The intent of this section is to outline the important of controls to prevent cyber-attacks and explain how weaknesses in controls and vulnerabilities can render these controls ineffective.

### 2.3.2 Requirements

The RTO shall:

a) document their control architectures.

b) identify possible vulnerabilities in controls, the modes of failure of these controls, means of detection of control failure and the impacts of control failure.

c) identify controls and vulnerabilities that could be introduced into their trusted network of organisations.

d) put in place processes to share knowledge about threats, vulnerabilities and incidents across their supply chain, including adding requirements for these processes into supplier and sub-contractor contracts.

e) implement management systems to ensure controls remain free of vulnerabilities over their lifetime or where vulnerabilities cannot be remediated, compensating controls are implemented, sufficient to bring total risk within accepted risk tolerances.

f) not rely on “security by obscurity”, where it is assumed hackers cannot obtain information about the security design, as a control.

g) not rely on physical isolation as the sole means of access control unless the design of the isolation is absolute including addressing system upgrades and maintenance and the effectiveness of the control has been rigorously tested.

### 2.3.3 Background and Rationale

ISO/IEC 27000:2014 defines a control as a measure modifying (cyber) risk and a vulnerability as a weakness in a control that can be exploited by a threat.

Vulnerabilities can exist in any control device, operational system, operational environment, procedures, controls or monitoring systems. All vulnerabilities will be identified for exploitation by hostile actors, to the extent that they can be identified and an exploit developed.

The effects from exploited vulnerabilities can be catastrophic given the scale of systems and the consequence of the manipulation of a system. Diligence is required by organisations in selecting and implementing controls, in each element of the system and stage of the engineering and operational lifecycle.

In this new era of business automation, interconnectivity and information dissemination, security shall be paramount and based on good-practice architectural principles and not rely upon “security by obscurity” or lack of connectivity. It shall be assumed that any system, physical or otherwise, has a level of risk of cyber-attack.

There are several characteristics of control systems and their vulnerabilities that are specifically relevant to rail. These include:

- The primary security control for many control systems is physical isolation. Vulnerabilities in physical isolation can be created by business requirements for:
  - Remote operations;
  - Remote support including by external suppliers;

  - Integration with other systems such as corporate applications;
  - Converged IT/OT operating models, where the same staff and management systems can be used to support both corporate and operational technologies;
  - Shared technology infrastructures, including use of private and public cloud services, and use of logical isolation.
- Rail systems are increasingly using corporate standard technologies, including standard desktop, server, and network equipment and software, and can be vulnerable to the same vulnerabilities that affect corporate technologies.
- Remediation of known vulnerabilities in rail systems may be delayed beyond the RTOs target time limit for many reasons, including:
  - Rail systems shall not have periodic scheduled maintenance during which vulnerabilities can be remediated, for example by updating vulnerable software;
  - Rail systems supplier shall not support or validate software updates or improved controls for use in rail systems;
  - Legacy or out-of-date technologies may not have any remediation available;
  - RTOs should not have adequate non-production verification environments to effectively validate changes prior to implementation in production;
  - Changes can affect certifications such as the Rail System's Safety Integrity Level, or may be deemed by regulators to constitute a material, reportable change in controls;
- Rail system components can be vulnerable to physical damage or interference where they are deployed in remote areas, or are accessible to the public.

## 2.4 Cyber Impacts, Safety and Resilience

### 2.4.1 Intent

This section addresses the potential impacts of cyber-attack and explains the need to maintain safety and resilience in rail operations.

### 2.4.2 Requirements

The RTO:

a) shall identify and assess the consequences of possible cyber-attack. The risk management plan shall explicitly identify and address both most-likely but also most-dangerous threats, ensuring that safety is always maintained and that operations are resilient in the face of common cyber-attacks.

b) should develop security architectures that exhibit characteristics of safety and resilience and review designs, and test effectiveness of these controls periodically.

c) shall not operate rail systems which cannot demonstrate safety characteristics where failure could have serious or catastrophic impact.

### 2.4.3 Background and Rationale

Cyber-attacks are events that can have a wide range of consequences for rail systems:

- injury or death of travellers, staff or the public;
- disruption to efficient operation;

- reputation damage;
- misinformation to public, stakeholders and suppliers;
- economic loss.

In calculating the impact of a threat/hazard, an organisation should consider not only the legal, economic and reputational impact of the immediate event, but also the impact on the broader industry and the public's confidence in transport systems. Maintenance of confidence in the safe operation of rail networks is an intrinsic goal of all RTOs.

The two essential security goals of critical infrastructure are safety and resilience are:

- **Safety** of rail operations shall be maintained always, so far as is reasonably practical (SFAIRP). Once a hacker is inside an operational network and potentially manipulating the information on which control systems rely, it is very difficult to ensure safe operation. For this reason, a deliberate bias in controls shall be taken in favour of prevention versus remediation and recovery.
- **Resilience** is the ability for the system to continue to function during and after a cyber-attack. Resilience needs to be assured against deliberate and non-deliberate acts. Resilience assists in achieving reliability and availability.

Safety and Resilience is improved by:

- reduction in the likelihood of successful attack through overlaying of independent control mechanisms (Defence in Depth) and active maintenance of controls (e.g. patching and testing of effectiveness);
- having systems in place to detect attack;
- diligent management and monitoring of systems to maintain operations and detect anomalies early, triggering appropriate responses as soon as possible;
- awareness of operational states - normal, contingency and recovery - and appropriate handling of other activities;
- reduction of disruption once systems come under attack – planning and staff response training is key to the management of incidents;
- effective collaboration with law enforcement agencies and other organisations during and after incidents improving the ability to mitigate the effect of attack, for example by network traffic control.

## 2.5 Risk assessment and management for critical infrastructure

### 2.5.1 Intent

This section addresses the need to have an integrated risk management plan that addresses cyber-security risk.

### 2.5.2 Requirements

The requirements are as follows:

a) Management shall implement a risk management plan for railway control systems, appropriate to the management of cyber security risks associated with these systems.

b) The risk management system should include:

- Threat analysis using a defined methodology (see 2.1.4);

- Controls that cover asset and risk identification, and incident prevention, detection, response and recovery;
- Multiple independent controls to prevent and detect each type of threat;
- Identification of risks that are outside of management's risk tolerances;
- A mandate that threat analysis and control assessment should be performed by suitability qualified and competent people with knowledge of control systems and cyber security;
- Formal acceptance of residual risk at the correct level of management;
- Specific action plans to bring risks to within tolerance, including who, what and when actions will be completed;
- A process to communicate and develop knowledge about risks;
- A process to regularly review risk plans considering changes to internal or external conditions (at least quarterly);
- Process to report on the risk plan status and effectiveness to the executive management and board regularly (at least quarterly).

### 2.5.3 Background and Rationale

Risk management is a key management tool to assist making decisions about investment priorities and the safety state of the railway. Risk management plans take an assessment of threat, controls and vulnerabilities and create specific action plans with assigned responsibilities for action and should be a continuous improvement process.

Risk shall be assessed and evaluated against acceptable limits (risk tolerance). Where risks are evaluated to be not within tolerance, additional controls should be put in place or controls enhanced to bring risks within tolerance. This continuous assessment, evaluation and adjustment of controls is called risk management, and is a core on-going management disciple in cyber security.

There are some distinctive characteristics of risk management of cyber security risks in the domain of rail. These include:

a) Rail cyber security risks may cause impacts to both cyber assets and the physical world, including to rolling stock, signalling, switching, and people. Impacts may include loss of safety and injury. As such, rail cyber security assessments should emphasise the ongoing reliable and safe operation of the system;

b) Consequences may be substantially higher than are seen in general corporate risk assessments, especially for risks that could result in loss of safety or injury. The RTOs risk methodology needs to accommodate and emphasise the importance of these high consequences;

c) The operational life of control systems is often many years, and it is likely that business requirements, cyber threats and vulnerabilities, and supporting systems will significantly change over this period. Rail cyber security controls will need to adapt over their lifetime to their environment.

Comprehensive and regular assessments of the risk management plan should consider:

a) Governance;
   - Are systems of review and assurance adequate?
   - Is management responsibility clearly defined?

- Is sufficient independence designed into the arrangements?
- Are legal requirements met?
- Are actions completed on schedule and delivering the expected improvements to controls?

b) Changes in the threat, goals or external environment;

c) Internal and external communications about the plan;

d) Planning (e.g., Emergency Response and Contingency Plans) and staff training;

e) Review of third party systems and devices – are the risks from third parties captured?

f) Internal system interfaces and inter-organisational interfaces;

- Are these identified and documented?

g) Current and future state of all operational systems are in line with their lifecycle management;

- Is risk assessed as part of any planned changes?
- Are systems maintained is a secure state?

h) Analysing changes between reviews and appropriate actions taken better manage critical infrastructure and coordinate activities.

## 2.6 Governance and the source of security requirements

### 2.6.1 Intent

This section addresses the requirement for organisations to formalise their governance arrangements for cyber-security and identify sources of security requirements.

### 2.6.2 Requirements

The RTO:

a) shall regularly (at least annually) review their policies, procedures and governance structure for managing cyber security.

b) Shall assign responsibilities throughout the organisation for cyber-security.

c) Should formalise specific accountability and responsibility for cyber-security in role descriptions / job specifications / policies.

d) should identify key internal and external stakeholders (which include customers, vendors, suppliers, service providers, government agencies etc.) and ensure they have input into governance processes and contribute to knowledge of systems, controls and vulnerabilities.

### 2.6.3 Background and Rationale

Governance is the responsibility of the executive management and board of the RTO. As a general principle governance responsibility, cannot be transferred, outsourced or avoided, and shall be managed by the RTO. There shall be executive level support and oversight of cyber-security.

The source of security requirements varies from organisation to organisation; however, these are the most common sources:

a) The requirement to maintain safety comes from occupational health and transport safety legislation;

b) Rail specific requirements come from rail industry and transport standards and is regulated via the national regulatory schemes for the industry;

c) Government-owned organisations, or suppliers to government, are often required to meet information security standards for government organisations;

d) Retention of information, for example CCTV, system logs, ticketing data, can be a requirement of federal and state legislation relating to reporting of criminal activity, inquests and retention of evidence;

e) Personal information protection requirements can impact ticketing, security systems and people and vehicle tracking system security requirements;

f) Payment industry security standards can impact ticketing systems security requirements;

g) Normative standards are a major source of control requirements;

h) Contractual commitments can create security control requirements;

i) Risk assessment can create security control requirements.

## 2.7 Assurance

### 2.7.1 Intent

This section addresses the requirement for organisations to formalise their governance arrangements for cyber-security and identify sources of security requirements.

### 2.7.2 Requirements

The RTO shall:

a) undertake a program of assurance which collects evidence to demonstrate the cyber-security of their systems, across technological, people, and process dimensions.

b) only approve systems for use which have evidence to demonstrate the cyber-security of their systems, where lack of security could result in a loss of safety.

c) only use suppliers who can demonstrate that their products and services demonstrate cyber-security suitable for the products and services they supply.

### 2.7.3 Background and Rationale

It is not sufficient to believe a system to be secure. Evidence shall be collected to demonstrate the effectiveness of the security controls.

ISO/IEC TR 15443 states that “assurance is related to the demonstrated ability of an entity to perform its security objectives. Assurance is determined from the evidence produced by the assessment process of an entity.”

Assurance requirements are determined by analysing the influencers of the system which can include such intangibles as politics, culture, local laws and mandated requirements.

Assurance methods can be categorized into three high-level approaches (ISACA):

a) Assessment of the deliverable, i.e., through evaluation and testing. In the development of safety-critical systems there shall be validation & verification (V&V) testing and behavioural testing e.g. penetration testing and fuzz testing. In assuring the deliverable, the RTO shall assess both the component and the total system as configured for operation;

b) Assessment of the processes used to develop or produce the deliverable (e.g. Software Quality Assurance including standards such as CMMI, and operate the system);

c) Assessment of the environment, such as personnel and facilities.

“Correctness assurance” refers to the assessment of the deliverable to verify the correct implementation per the design. In contrast, “effectiveness assurance” for security assesses the suitability of the deliverable’s security functions to counter the perceived or identified threats.

When purchasing products and services organisations rely on independent evaluation of technology. Preference should be given to use of Common Criteria (CC) and formally evaluated products over unevaluated products and services. In reviewing certifications and third-party assurance, it is important to look at what has been the scope of the assessment and determine if this is sufficient for the current purpose.

In addition to technology products, it is also a requirement to implement assurance processes on data where this controls the operation of the rail control system. Where external data sets and messages are introduced into the ICS it is a requirement to build data quality assessment into the ingestion process.

An analysis of assurance strategies for ICS systems can be found in Knowles et al (2015).

Knowles, William, Jose M. Such, Antonios Gouglidis, Gaurav Misra, and Awais Rashid. "Assurance techniques for industrial control systems (ics)." In *Proceedings of the First ACM Workshop on Cyber-Physical Systems-Security and/or PrivaCy*, pp. 101-112. ACM, 2015.

# 3 Protecting Rail Control Systems

## 3.1 Principles of effective cyber security design

The standard includes five architecture principles of cyber security control design that should be adopted by RTOs:

i. ‘If it is not secure, it is not safe’: States of safety shall be derived from security considerations.

ii. Proportionate Response: Measures shall be appropriate to the risk being considered but not hinder rail operations.

iii. Goal-based Security: Establishing goals rather than initiatives ensures more pervasive security and organisation adoption.

iv. Designed-in Security: Security should be at every level of design and development and never seen as a “bolt on”.

v. Defence-in-Depth: For each threat there should be multiple independent overlapping controls.

The five principles shall be applied as a set. Where there is tension or contradiction between Principles 1 and 2, the ‘tie’ shall be resolved in favour of Principle 1 (i.e. safety first).

In addition, this section identifies eight design principles in secure systems design, based on the work of Saltzer and Schroeder (1975).

### 3.1.1 Principle 1: If it’s not Secure it is not Safe [Is-safe]

**Statement:** An insecure system is not a safe system.

**Rationale**: Unsecured systems can become targets for malicious acts or non-deliberate compromise, and thereby trigger safety events or accidents. Failure to secure systems can contravene regulatory safety requirements.

Therefore, a system shall be secure to be considered safe. Security should be viewed as a facet of safety; security and safety are highly dependent and interrelated.

**Implications:** An understanding of safety shall include security considerations and a safe system shall be protected from cyber-threats through selection and implementation of controls.

There shall be processes to ensure controls remain free of vulnerabilities and remain effective.

A safe system shall withstand successful attack, failing in a way that is safe. Use of Failure Modes Analysis can assist in the analysis of how the system will behave when attacked and compromised.

### 3.1.2 Principle 2: Proportionate Controls [Proportionate]

**Statement:** Security controls shall always be considered proportionate to the likelihood and consequences of a vulnerability being exploited.

**Rationale:** As security is integral to any system – by Principle 4 – controls should not be perceived by users and stakeholders as being too onerous or adding no value. Otherwise, users will by-pass controls.

**Implications:**

- The Most Likely and Most Dangerous threats shall be managed actively, and controls shall be prioritised to reduce these risks.
- Controls that do not significantly improve risk and which impact adversely on stakeholders should be avoided.
- When choosing between control options that have the same, preference should be given to those with greater usability (from a customer and operator perspective).
- Note that legislative and regulatory (i.e. mandatory) requirements sometimes override this principle.

### 3.1.3 Principle 3: Goal-based Security [Goal-Based]

**Statement:** Security control requirements should be derived from higher-level security objectives that link to business objectives. These should be clearly articulated as Security Goals.

**Rationale:** Technology focused security initiatives with no traceability back to business objectives, strategies, and policies are likely to be unsupported by the broader business.

A coherent and integrated set of security goals makes the rationale for control measures more transparent and supports consistent investment.

Tactical or niche security initiatives can sometimes be effective however they risk not integrating in the broader security of the organisation.

**Implications:**

- Organisations shall identify, endorse and communicate their security goals;
- Organisation should consider adoption of an enterprise security architecture to ensure an integrated and consistent approach to controls identification and design. This should be aligned with enterprise architecture (EA) frameworks adopted by the organisation or

where a security architecture framework is adopted (e.g. SABSA), a mapping to the EA frameworks in use should be provided;

- When identifying control objectives and controls, architects should explicitly link these to the overarching security goals of the organisation;
- Solution Architectures developed for specific projects or systems should be mapped to the Security Goals and Enterprise Security Architectures of the organisation.

### 3.1.4 Principle 4: Design-in Security [Design-In]

**Statement**: Security considerations must be integral to the design, development, installation and operation of any system.

**Rationale**: Security is a business requirement and so shall be treated like any other mandatory requirement – not tacked on as afterthought. It is a fundamentally hard problem to add security to an insecure system, post hoc.

**Implications**:

- Designs should exhibit clear evidence of inclusion of security goals in requirements;
- When systems are implemented, demonstration of the effective operation of security controls shall be part of the system certification and its accreditation to operate;
- Any system that requires technical security mechanisms to be overlaid onto it to achieve minimum acceptable risk shall either be:
    a) discouraged from use, or
    b) well isolated and monitored, if there is no alternative to its use.

### 3.1.5 Principle 5: Defence-in-depth [Defence-in-Depth]

**Statement:** Security shall be based around multiple overlapping independent controls for each threat.

**Rationale:** No single control can be made 100% reliable: zero- day or unpublicised vulnerabilities; poor deployment and configuration practises; and poor operational practises can all reduce, or nullify, a control's effectiveness. Therefore, it is better to expect that a security control will fail and to design for it.

**Implications:**

- For each threat there should never be a reliance on a single control e.g. you should not rely on user access-control as the sole means of preventing unauthorised access to a system.
- For each threat there should not be functional dependence between the controls e.g. if you are relying on network segregation and network access control and event logging controls for security then you should not rely on a single firewall to perform these functions.
- You should perform Failure Mode Analysis to understand the effect of subsystem/component failure.
- Cyber security controls need to span people, process, and platforms and not be purely technical but address the behaviour of users and administrators.
- In defending from a threat, the set of controls should achieve the following objectives:
    - Prevention – multiple controls should prevent intrusion;

- Containment – where a hacker can bypass a perimeter control, the hacker should not have access to the full system but rather a locked-down interface layer requiring user authentication;
- Detection – Controls should be in place that allow detection of abnormal activity and reporting of that activity. It is important that these detection controls are protected from disablement and modification;
- Response – Controls should allow security administrators to respond to, investigate, record and adjust controls in response to a suspected cyber-incident;
- Recover – Where an attack can disable or damage systems, it should be possible to isolate and restore systems to an operational and secure state within defined ttimeframes.

### 3.1.6 Other Design Principles (Saltzer and Schroeder's design principles)

Saltzer and Schroeder (1975) provide eight (8) examples of design principles that apply to protection mechanisms:

a) Economy of Mechanism: keeping the design small and simple reduces the complexity and potential for unwanted access paths;

b) Fail-Safe Defaults: assuming that the default rule is to provide "lack of access" allows for simplified explicit declarations to "allow access";

c) Complete Mediation: forces a system-wide view of access control, which extends beyond normal operational modes by also considering initialisation, recovery, shutdown and maintenance;

d) Open Design: by not making the design secret it does not depend upon lack of knowledge from hackers (which they can gain) but more the robustness of the design with protected keys;

e) Separation of Privilege: protection mechanisms should require multiple keys;

f) Least Privilege: (like Fail-Safe Defaults) system and user account privileges should explicitly allow access from a system-wide default state of "access denied";

g) Least Common Mechanism: functions should be used under each user's privilege and not utilise supervisor accounts, nor common variables that could be manipulated to divert usage;

h) Psychological Acceptability: simple and clear design of user interfaces allow users to comply with protection mechanisms and not seek shortcuts that could circumvent controls or privileges without knowledge;

## 3.2 Effective Cyber security

### 3.2.1 Intent

This section addresses the requirement for organisations manage security across the five NIST Cybersecurity Framework functions.

### 3.2.2 Requirements

The RTO:

a) shall have a security management system that addresses the five functions of the NIST Cybersecurity Framework: identify, protect, detect, respond, recover.

### 3.2.3 Background and Rationale

There are five key functions of security that work together to ensure cyber security. These should be considered an interlocking set or matrix of functions, rather than a sequence or activities.

#### 3.2.3.1 Identify

The Identify function seeks to correctly Identify and assess what kinds of business process, data sets and systems (assets) need to be protected. This should be done considering organisational mission, objectives and goals. Organisational understanding should be at the centre of identifying at risk systems. Managers and actors should agree on what systems are required to be protected. Following this, a threat assessment exercise should be undertaken to assess their threats and vulnerabilities.

#### 3.2.3.2 Protect

Assets need effective protection from threats after they have been identified as being at risk. Certain operational IT and security activities will be seen as being 'at risk' and require effective controls to be protected as well. The Protect function seeks to stop bad actors from gaining access to and damaging these assets and disrupting business operations.

#### 3.2.3.3 Detect

Most successful cyber-attacks are not detected in a timely manner. Operations require ongoing observation and monitoring to identify abnormal activity. The purpose of this function is to have an ongoing system in place to detect and monitor the cyber security landscape, both external to the organisation and internal to the networks and systems being protected. Having this function helps to be proactive instead of reactive.

#### 3.2.3.4 Respond

The response function is what happens in the event of a breach. These are specific risk management strategies that are used to respond to an attack. These activities are based on previously created plans and incident response tactics. Effective response can ensure the impact of cyber-attack is minimised.

#### 3.2.3.5 Recover

The recover function includes strategies and operational processes that restore services after a breach. The purpose of recovery function is to restore the services as they are required. These are important as they ensure a robust, comprehensive and speedy response to security events and incidents. Recovery is dependent on protecting the underlying data and systems configurations from attack and using these to restore systems to pre-attack condition.

## 3.3 Training

### 3.3.1 Intent

This section addresses the requirement for RTOs to ensure their people are trained.

### 3.3.2 Requirements

The RTO:

a) shall implement a comprehensive cyber-training and education program.

### 3.3.3 Background and Rationale

People and process form a significant element of cyber-security controls. Human's also are a source of vulnerabilities, in that their knowledge is not complete and judgement is often imperfect. Hackers use this to socially engineer access to systems.

Training activities for cyber security should be comprehensive and seek to develop skills across the organisation. These should include:

i) Developing, evaluating and implementing cyber secure systems from an enterprise perspective. This involves securing communication channels, networks, data, and control and information systems;

j) Threats and vulnerabilities relevant to industrial control systems. CERT Australia provides an industry resource in this domain of knowledge;

k) An understanding of security frameworks and standards e.g. the NIST framework;

l) Education on how to develop security architectures that are comprehensive and goal-oriented;

m) How to develop and implement policies that are adaptive, proactive and designed to stand up against cyber-attacks;

n) Skills in communicating complex technical information to policy makers who cannot be across the latest in cyber security problems;

o) Develop skills in developing and using security information management and event management systems to discover new threats and analyse them;

p) Technical skills in the operation of security tools;

q) Training in analysing complex information to identify problems, analyse solutions and make judgements require solutions;

r) Processes and skills to respond to security incidents;

s) Generating solutions to critical breaches through innovative solutions;

t) Developing core skills around cyber security breaches in order to generate effective responses and innovative solutions;

u) Learning to work in teams, working autonomously to respond effectively and quickly to emerging threats;

v) Training to all staff and contractors to raise their awareness of the cyber threat and good cyber-safety practices.

Training programs should reflect the holistic nature of the problems emerging from cyber security. They should not just focus on effective control systems but also be focused on both the critical thinking, problem solving and strategic aspects of cyber security. Training should be at both the individual and team level.

## 3.4 Management Support and Funding

### 3.4.1 Intent

This section addresses the requirement for organisations to ensure that cyber security has sufficient management support and funding.

### 3.4.2 Requirements

The RTO:

a) shall demonstrate their support for cyber-security, and shall ensure there is sufficient funding for cyber security functions and activities though their executives and board.

### 3.4.3 Background and Rationale

The best technical designs will be rendered ineffective overtime if sufficient priority and resources are not made available to create a secure context in which they operate. For this reason, boards and executive support is vital.

The executives and board of the organisation demonstrate their support for cyber security by the following key actions:

- Formal recognition of the importance of cyber-security in organisational policies;
- Making sure that improving cyber-security is given adequate priority in corporate strategies and operational plans;
- Ensure adequate funding for cyber security;
- Establishing organisational structures that are responsible and accountable for information security with clear lines of reporting with sufficient independence from operational management;
- Allocating responsibilities for cyber security in staff's job standards and in supplier's contract conditions;
- Requiring that all projects address cyber security goals and requirements;
- Maintaining an active interest in the operation of cyber-security and requiring regular board-level reporting (at least every 6 months) on security risk and management system effectiveness;
- Requiring regular cyber security training for all staff in the organisation.

## 3.5 Cyber Security in the Systems Lifecycle

### 3.5.1 Intent

This section addresses the requirement for organisations to build-in security into all phases of the system lifecycle.

### 3.5.2 Requirements

The RTO:

a) shall include security and requirements into all stages of a systems lifecycle: systems requirements, design, development and delivery activities (including methods for validation and verification of security), commissioning, operations, decommissioning and disposal.

b) should re-evaluate security controls when systems are being upgraded, updated and maintained to determine if current controls are effective and if additional controls should be introduced.

### 3.5.3 Background and Rationale

#### 3.5.3.1 Security Requirements and Procurement

Security requirements need to be considered in any new system, as well as how well a new system would integrate into the existing environment.

Similar for systems development should be used for procurement:

- **Design**: modern protocols and architectures should be used that have achieved standardisation and have acknowledged security methods.
- **Development**: modern development tools should be used that support secure methods for systems development and verification, including tools for code analysis, fuzzing and automated regression testing for common vulnerabilities.
- **Installation**: existing security functions should not be hampered or compromised by the introduction of a new system or the upgrade to an existing system, additionally security should be established as part of installation rather than after the fact. Production verification testing shall be performed with security enabled.
- **Maintenance**: regular maintenance shall be undertaken including the application of regular and timely patching of vulnerabilities. In addition, provision for upgrading security to meet new threats for the duration of the systems life should be included in the integrated maintenance program contractual requirements.
- **Decommissioning and Disposal**: all system and device disposal should be done to prevent any analysis by an unauthorised party.
- **Independent Validation and Verification**: the role of, and requirement for, independent validation should be enshrined in the contract.
- **Provision of evidence:** a key requirement is any contract should be the requirement for the vendor to provide evidence to support security control effectiveness and compliance activities, during the system's life. These requirements should be included in contract requirements and service level agreements.

The US Department of Homeland Security has developed a document "Cybersecurity Procurement Language for Control Systems" which can assist in specifying security requirements for vendors.

#### 3.5.3.2 Systems Design

Designers should adopt the principles of effective cyber security design (Section 3.1). This ensures security needs will be considered throughout the initial design, system architecture, development activities, environment integration to common services (e.g., user provisioning, de-provisioning, maintenance, authentication, authorisation and accesses control) and operations monitoring mechanisms.

Threat and failure mode analysis, combined with compliance with standards, is the primary source of system security requirements. Support for operational security should be built into the design from the ground up.

When considering device and interface communications, modern technologies such as TCP/IP, MODBUS and other common protocols should be chosen instead of proprietary technologies. This enables the use of standard security mechanisms and systems and moves away from approaches such as "security by obscurity".

System interfaces and boundaries are places where design, development and configuration errors can create security vulnerabilities. Designers shall therefore, as well as including controls for integrity and available for general safe operation, include controls that guarantee the integrity, availability and non-repudiation of messages and communication between systems.

A balance between over-the-air and hard-wired connectivity and communications should be considered so physical access would be required to gain full operational control of a RCS.

While designs shall never rely on security-through-obscurity, details of security designs and configurations should be protected from loss of confidentiality and treated as a security asset requiring protection. Security aspects of designs, including points of integration for systems within operational monitoring mechanisms, should not be released publicly unless the security is a requirement for effective integration. If this is required, the level of detail should be reviewed to only show what is necessary, and the audience should be tightly controlled and readership recorded for later review if required.

#### 3.5.3.3 Systems Development

A recognised secure software development standard should be chosen and should address:

- threat modelling and architectural risk analysis;
- attack surface reduction;
- 'fuzz' testing (automated software testing using invalid, unexpected or random data);
- static analysis.

Software quality assurance techniques assist in adhering to a chosen secure development process and maintain the focus towards reducing the attack surface of systems being developed.

If development is being conducted externally then such standards and security requirements should be specified and adherence to process and product quality standards evaluated.

Compliance to normative security controls for procurement (ISO 27001, ISO 27002), risk assessment (ISO 27005) and quality standards (ISO9001) should be adopted for all procurement activities, and staff trained in the assessment of security requirements and suitability of supplier security mechanisms. Where sufficient skills in assessment are not available within the organisation, expertise should be independently procured.

#### 3.5.3.4 Installation

Installation of new systems or upgrades shall not introduce vulnerabilities or compromise into the current environment. A review of the latest security assessment of the product should be undertaken before approval for installation to ensure installation will not degrade security. This should also include a review of security mechanisms used by a new or upgraded system to assess if improved security mechanisms can be utilised.

It should be assumed that all new equipment and systems might contain mechanisms for compromising cyber security. Therefore, supplier disclosure should include:

- required remote network access for operation;
- supplier remote access (e.g., maintenance);
- supplier requirement to update functionality or common data;
- supplier requirement to retrieve data (e.g., logs or configurations) remotely;
- equipment requiring data to be sent to the supplier (e.g., profiling data);

- supplier access to re-program a system or device.

If any of the above are required, then a risk analysis should be undertaken for formal review and acceptance by management. Additional, security mechanisms should be implemented to monitor such communications for abnormal use.

As each installation is undertaken appropriate Emergency Response and Contingency Plans should be completed/updated and staff understanding and training acknowledged. These plans should also be tested regularly in training exercises to evaluate adequacy and assist in further understanding of organisational resiliency.

Common architectural (also appropriate for existing systems) considerations should include:

- device and user authentication, authorisation and access control (AAA);
- monitoring and alerting of privileged access, failed logons, and unusual access patterns;
- Monitoring of systems resources and network usage;
- Malware and protection from unauthorised change;
- White-listing applications and processes;
- Network segmentation and firewalling;
- Host-firewalls and services listening on IP ports;
- Cryptographic management;
- Remote management;
- Availability and integrity of security subsystems and data.

Once new systems and equipment are operational they should be regularly (at least annually) included in routine penetration testing by “white hat” or “ethical hacking” service providers. Procedures should be developed to allow this testing to occur on operational systems in such a manner that they achieve meaningful test coverage yet do not pose a risk to the reliability, availability, maintainability or safety of rail operations.

#### 3.5.3.5 Maintenance

Maintenance of security shall be included in the integrated maintenance plan for the RCS. It is not acceptable to have an operational system with a maintenance plan which does not ensure timely (relative to the risk) patching of critical vulnerabilities or the application of compensating controls.

Poor patch and vulnerability management is a source of system vulnerabilities and loss of system integrity. A procedure shall be in place that manages the risks of patching (e.g. unplanned outages) but which ensures:

a) that patching is timely; and

b) management are aware of current patching levels and vulnerability status.

Records of maintenance shall be maintained.

After the completion of each maintenance task(s) testing should be performed to ensure correct operation and verification that vulnerabilities have not been introduced. Test results should be compared historically to ensure continued correct operation of systems and equipment as well as the detection of any anomalies.

System update planning should consider system tools, support and monitoring software as well as applications.

#### 3.5.3.6 Decommissioning and Disposal

All systems and equipment should be disposed in a secure manner to limit analysis by any third parties, whether external or internal. These disposal activities should include abandoned, destroyed, as well as decommissioned equipment and all data storage media.

#### 3.5.3.7 Independent Validation and Verification

Independent evaluations (Validation and Verification) of the security mechanisms on safety-critical systems must be undertaken at least annually and as part of any installation or major upgrade. Evaluations should follow an agreed scope and reference the architectural design of the environment to ensure commonality in reporting, providing historical correlation of results even if different external vendors are selected. If it is not practical to fully test all controls during each testing cycle, a program of testing should be implemented that ensures all controls are tested over time with more critical controls tested more frequently.

After each evaluation, a remediation plan should be produced and endorsed by management that addresses any issues identified. The status of remediation should be included in routine management reporting on security status.

# 4 Handling threats and incidents

## 4.1 Intent

This section addresses the requirement for organisations to effectively handle current threats and incidents.

## 4.2 Requirements

The RTO:

a) shall have a demonstrated ability to respond to cyber-incidents without loss of safety and for common types of incidents, without disruption to services.

b) should have an ability to respond to heightened threat levels or anticipated attack via graduated levels of alert with increased protective and response postures.

c) should have a cyber incident response plan that is integrated and coordinated with overall organisational and sectoral service continuity, crisis and public safety plans and that includes interfaces with relevant external agencies.

## 4.3 Background and Rationale

The general steps in responding to a cyber-attack are:

- Prepare – develop the capability to respond. This occurs prior to the attack;
- Identification – determine if an incident has occurred;
- Containment – limiting the damage;
- Eradication – remove the cause of the damage;
- Recovery – restore services to normal operational status;
- Lessons Learned – Reflect on and learn from the incident.

Regular testing of organisational capabilities should be undertaken through rigorous training exercises. The performance and results should be analysed for opportunities for improvement

### 4.3.1 A rise in threat level or unexpected attack

RTOs need to establish a formal policy and procedure for handling of threats and incidents. This policy should include the concept of levels of threat/emergency. For example, the following is adapted from the UK Department for Transport (DfT) to the Australian context:

**Level 0: Steady State**

This is the normal operational state where normal monitoring occurs, and from where escalation should originate from to ensure a base-state snapshot is available of all environment elements before they were compromised.

**Level 0: Exceptional Occurrence**

Although still a level 0 state due to no active breaches, this level should be triggered when greater rigour is required due to external (public) interest or government/international collaborations are underway and therefore require more information for active communications.

**Level 1: Significant Emergency**

This should be the first active investigation and response state that has been triggered due to event. This could be caused by:

- degradation of operational networks
- exfiltration of data and intellectual property
- media reports that undermine trust in operational capabilities.

**Level 2: Serious Emergency**

Once a breach or other cyber incident is suspected, notification should be given to the Australian Cyber security Centre and CERT Australia. Detailed information should be collected and submitted in order for the correlation of the incident with other events through Australian government agencies and businesses. Incidents that trigger such a level should include events that disrupt public services as well as public events — all of which should be monitored to control media reports.

**Level 3: Catastrophic Emergency**

Incidents that result in the loss of critical services, or the loss of a single essential service for a sustained period, should be considered a Catastrophic Emergency. The procedures should follow the same as Level 2 with additional resources provided for coordinated communication and collaboration of activities.

All incidents should be reported to the Australian Cyber Security Centre and CERT Australia for national awareness and assistance in a coordinated national response. Subsequent actions should also be undertaken in collaboration, including responses to media enquiries.

In the event of a cyber-attack, it is likely that a crime has been committed. The RTO shall have procedures and established points of contact with local police to notify them of suspected cyber-crimes.

Care should be undertaken when providing any media statements or responding to any external enquiries as there could be a high risk of reputational damage and loss of confidence in the rail system. Crisis management plans should identify roles and responsibilities for public communication in the event of cyber-attack.

### 4.3.2 Contingency in the event of a cyber attack

Immediate assistance shall be given to the safety of people who could be affected by the incident.

Once safety is established the RTO can look at continued operations. This may include:

- Starting limited, degraded operations where safety is established;
- Returning the network to normal operations;
- Taking remedial action to secure networks/systems where the point of breach is known;
- Identifying, isolating and preserving evidence;
- Internal investigations of how the breach occurred;
- Remedial action to prevent future breaches.

# 5 Implementing the Cyber Security Framework for Rail

## 5.1 Intent

This section addresses the requirement for organisations to adopt a recognised framework or standard for managing cyber-security and explains why the rail industry, via this Standard, has adopted the NIST Cybersecurity framework as the basis for industry reporting and benchmarking.

## 5.2 Requirements

The RTO shall:

a) adopt a formalised industry framework or Standard for managing cyber security.

b) shall map their cyber security management systems to the NIST Framework for Improving Critical Infrastructure Cyber Security and use this for reporting to industry regulators and in industry benchmarking activities, including the ability to report on maturity (Appendix B).

## 5.3 Background and Rationale

It is important that RTOs adopt a rigorous approach to managing cyber security. Home-grown or domestic standards rarely provide an effective basis for regulation, benchmarking and are difficult to externally assure. For this reason, this standard requires RTOs to adopt a recognised, relevant and appropriate framework for their cyber security management systems. Examples include:

- The NIST Framework for Improving Critical Infrastructure Cybersecurity;
- ISO 27000;
- ANSI/ISA-62443.

The NIST Framework for Improving Critical Infrastructure Cybersecurity is a framework used to manage, assess, and develop cyber security risk management profiles. It's internationally recognised as a world class approach to cyber security. The NIST Framework is used for the following reasons:

a) To describe the current state of cyber security in an organisation;

b) To create a 'target state' for cyber security;

c) To identify ways to improve based on a continuous quality improvement circles;

d) Assess and move towards the target state;

e) Create communication flows for the organisation to share knowledge about cyber security hazards.

The NIST Framework is a complementary strategy to an organisations cyber security program. The purpose of this framework is to use it as a type of benchmarking and quality improvement tool that can enhance cyber security.

A detailed explanation of the framework is beyond the scope of this standard however this Standard contains one resource that assist in its adoption in RTO:

- Appendix B: A Cyber Security Maturity Assessment Tool (normative) contains a tool that allows a holistic scoring of cyber-security maturity, for purposes of management and regulatory reporting and industry benchmarking.

## Appendix A Cyber security Hazards

| Hazard Number | Hazard | Heading Number |
|---|---|---|
| 1 | Attacks on the power supply chain – over and under supply | 2.1.3, 2.2 |
| 2 | Unauthorised physical access to control systems components, allowing hackers to disable, modify or access OT systems. | 2.1.3, 2.2 |
| 3 | Vulnerabilities introduced by joining Operational Technology (OT) and Information Technology (IT) environments, leading to improper separation and the ability to compromise integrity and availability of rail and train systems. | 2.2.3 |
| 4 | OT environment connected to the Internet, or a public network, leading to the ability to compromise integrity and availability of train and rail control systems | 2.2.3 |
| 5 | Insecure processes and practices for remote access and configuration management lead to systems being vulnerable to the installation of malware during routine maintenance and upgrades. | 2.2, 3.5.3.1, 3.5.3.4, 3.5.3.5 |
| 6 | OT environment connected to insecure network access points (e.g. WiFi) leading to the ability to compromise integrity and availability of train and rail systems | 3.5.3.4 |
| 7 | Hackers able to compromise supply chain partners' systems giving them knowledge of, or access to, OT systems. | 2.1.3.2,2.5.2, 3.5.3.1 |
| 8 | Lack of isolation from IT and OT environments, allowing attack vectors from IT into OT environment. | 2.2.3 |
| 9 | Ability for hackers to socially engineer access via targeting staff with dual access to IT and OT systems (due to lack of training and/or lack of technical controls). | 3.3 |
| 10 | Ability of hackers to impersonate staff due to theft of user name and password credentials via network sniffing. | 3.5 |

| Hazard Number | Hazard | Heading Number |
|---|---|---|
| 11 | Hackers able to install malware or modify configurations due to lack of configuration controls and access controls. | 3.5 |
| 12 | Hackers able to attack OT systems because of underlying vulnerabilities of COTS components or inadequate patch management. | 2.2 |
| 13 | Hackers able to disrupt operations due to inadequate organisational response. | 4 |
| 14 | Hackers able to disrupt systems because type of attack was not considered in original design of the system i.e. lack regular review and upgrading of security controls. | 2 |
| 15 | Hackers able to disable OT systems via deleting or encryption of information, due to inadequate access control and lack of isolated backup or system image and configurations. | 3.2.3.5 |
| 16 | Hackers able to cause panic by unauthorized access to passenger management systems. | 2.1.3.3. |
| 17 | Hackers able to create disruption to rail networks by eliciting an inappropriate and excessive incident response. | 4 |
| 18 | Hackers able to seize control of entire systems due to not being detected inside the OT network because of inadequate network monitoring. | 3.2 |
| 19 | Systems are unsafe because they cannot demonstrate a secure design and implementation. | 3.1.1 |
| 20 | Systems are unsafe because they cannot demonstrate secure operation, because controls are disabled, ineffective or untested. | 2.6 |
| 21 | Lack of controls on staff and contractors (e.g. monitoring of privileged access, lack of personnel vetting and monitoring, loose culture in engineering teams, unsupervised access) allow a malicious insider attack. | 2.1.3.2, 3.1.6, 5 |

## Appendix B Cyber security Maturity Assessment Tool

An assessment tool allows an organisation to self-assess the maturity of its risk-based approach to managing cyber threats. The below tool shall be used by all RTO to assess and report cyber security risk management maturity.

For each sub-category of the NIST Cybersecurity Framework:

Step 1 Assess current tier level from 1 to 4 for each sub-category

1: Partial
- ad hoc or limited processes,
- No systematic risk management

2: Risk Informed
- Security processes in place for areas of identified risk
- Policy and procedures developed
- Comprehensive application of risk management

3: Repeatable
- Security processes applied consistently with few lapses
- Security responsibilities defined and applied
- Staff trained

4: Adaptive
- Collaborative whole-of-supply-chain approach
- Continuous improvement
- Active engagement with external sources of knowledge
- Decision make based on empirical information

Step 2 Calculate Delta i.e. Current Tier – Target Tier

Step 3 Multiple Delta by Weight to produce Score

Step 4 Sum all scores in a category to produce category score and sum all scores to produce total maturity score

How to use:

Every 12 months (or more frequently if desired) perform this assessment and record the score by date to create trend line graphs of improvements. To identify areas of focus, calculate and record scores at the category level as well.

| Function | Category | Sub-Categories | Current Tier (A) | Industry Target (B) | Delta C=(A-B) | Weight (D) | Score C x D |
|---|---|---|---|---|---|---|---|
| Identify (ID) | Asset Management (ID.AM) | ID.AM-1 | | 3 | | 1.00 | |
| | | ID.AM-2 | | 3 | | 1.00 | |
| | | ID.AM-3 | | 3 | | 1.00 | |
| | | ID.AM-4 | | 3 | | 1.00 | |
| | | ID.AM-5 | | 3 | | 1.00 | |
| | | ID.AM-6 | | 3 | | 1.00 | |
| Identify (ID) | Business Environment (ID.BE) | ID.BE-1 | | 3 | | 1.00 | |
| | | ID.BE-2 | | 3 | | 1.00 | |
| | | ID.BE-3 | | 3 | | 1.00 | |
| | | ID.BE-4 | | 3 | | 1.00 | |
| | | ID.BE-5 | | 3 | | 1.00 | |
| Identify (ID) | Governance (ID.GV) | ID.GV-1 | | 3 | | 1.00 | |
| | | ID.GV-2 | | 3 | | 1.00 | |
| | | ID.GV-3 | | 3 | | 1.00 | |
| | | ID.GV-4 | | 3 | | 1.00 | |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| Identify (ID) | Risk Assessment (ID.RA) | ID.RA-1 | | 3 | | 1.00 | |
| | | ID.RA-2 | | 3 | | 1.00 | |
| | | ID.RA-3 | | 3 | | 1.00 | |
| | | ID.RA-4 | | 3 | | 1.00 | |
| | | ID.RA-5 | | 3 | | 1.00 | |
| | | ID.RA-6 | | 3 | | 1.00 | |
| Identify (ID) | Risk Management Strategy (ID.RM) | ID.RM-1 | | 3 | | 1.00 | |
| | | ID.RM-2 | | 3 | | 1.00 | |
| | | ID.RM-3 | | 3 | | 1.00 | |
| Protect (PR) | Access Control (PR.AC) | PR.AC-1 | | 3 | | 1.00 | |
| | | PR.AC-2 | | 3 | | 1.00 | |
| | | PR.AC-3 | | 3 | | 1.00 | |
| | | PR.AC-4 | | 3 | | 1.00 | |
| | | PR.AC-5 | | 3 | | 1.00 | |
| Protect (PR) | Awareness and Training (PR.AT) | PR.AT-1 | | 3 | | 1.00 | |
| | | PR.AT-2 | | 3 | | 1.00 | |
| | | PR.AT-3 | | 3 | | 1.00 | |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| | | PR.AT-4 | | 3 | | 1.00 | |
| | | PR.AT-5 | | 3 | | 1.00 | |
| Protect (PR) | Data Security (PR.DS) | PR.DS-1 | | 3 | | 1.00 | |
| | | PR.DS-2 | | 3 | | 1.00 | |
| | | PR.DS-3 | | 3 | | 1.00 | |
| | | PR.DS-4 | | 3 | | 1.00 | |
| | | PR.DS-5 | | 3 | | 1.00 | |
| | | PR.DS-6 | | 3 | | 1.00 | |
| | | PR.DS-7 | | 3 | | 1.00 | |
| Protect (PR) | Information Protection Processes and Procedures (PR.IP) | PR.IP-1 | | 3 | | 1.00 | |
| | | PR.IP-2 | | 3 | | 1.00 | |
| | | PR.IP-3 | | 3 | | 1.00 | |
| | | PR.IP-4 | | 3 | | 1.00 | |
| | | PR.IP-5 | | 3 | | 1.00 | |
| | | PR.IP-6 | | 3 | | 1.00 | |
| | | PR.IP-7 | | 3 | | 1.00 | |
| | | PR.IP-8 | | 3 | | 1.00 | |
| | | PR.IP-9 | | 3 | | 1.00 | |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| | | PR.IP-10 | | 3 | | 1.00 | |
| | | PR.IP-11 | | 3 | | 1.00 | |
| | | PR.IP-12 | | 3 | | 1.00 | |
| Protect (PR) | Maintenance (PR.MA) | PR.MA-1 | | 3 | | 1.00 | |
| | | PR.MA-2 | | 3 | | 1.00 | |
| Protect (PR) | Protective Technology (PR.PT) | PR.PT-1 | | 3 | | 1.00 | |
| | | PR.PT-2 | | 3 | | 1.00 | |
| | | PR.PT-3 | | 3 | | 1.00 | |
| | | PR.PT-4 | | 3 | | 1.00 | |
| Detect (DE) | Anomalies and Events (DE.AE) | DE.AE-1 | | 3 | | 1.00 | |
| | | DE.AE-2 | | 3 | | 1.00 | |
| | | DE.AE-3 | | 3 | | 1.00 | |
| | | DE.AE-4 | | 3 | | 1.00 | |
| | | DE.AE-5 | | 3 | | 1.00 | |
| Detect (DE) | Security Continuous Monitoring (DE.CM) | DE.CM-1 | | 3 | | 1.00 | |
| | | DE.CM-2 | | 3 | | 1.00 | |
| | | DE.CM-3 | | 3 | | 1.00 | |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| | | DE.CM-4 | | 3 | | 1.00 | |
| | | DE.CM-5 | | 3 | | 1.00 | |
| | | DE.CM-6 | | 3 | | 1.00 | |
| | | DE.CM-7 | | 3 | | 1.00 | |
| | | DE.CM-8 | | 3 | | 1.00 | |
| Detect (DE) | Detection Processes (DE.DP) | DE.DP-1 | | 3 | | 1.00 | |
| | | DE.DP-2 | | 3 | | 1.00 | |
| | | DE.DP-3 | | 3 | | 1.00 | |
| | | DE.DP-4 | | 3 | | 1.00 | |
| | | DE.DP-5 | | 3 | | 1.00 | |
| Respond (RS) | Response Planning (RS.RP) | RS.RP-1 | | 3 | | 1.00 | |
| Respond (RS) | Communications (RS.CO) | RS.CO-1 | | 3 | | 1.00 | |
| | | RS.CO-2 | | 3 | | 1.00 | |
| | | RS.CO-3 | | 3 | | 1.00 | |
| | | RS.CO-4 | | 3 | | 1.00 | |
| | | RS.CO-5 | | 3 | | 1.00 | |
| Respond | Analysis (RS.AN) | RS.AN-1 | | 3 | | 1.00 | |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| (RS) | | RS.AN-2 | | 3 | | 1.00 | |
| | | RS.AN-3 | | 3 | | 1.00 | |
| | | RS.AN-4 | | 3 | | 1.00 | |
| Respond (RS) | ion (RS.MI) | RS.MI-1 | | 3 | | 1.00 | |
| | | RS.MI-2 | | 3 | | 1.00 | |
| | | RS.MI-3 | | 3 | | 1.00 | |
| Respond (RS) | Improvements (RS.IM) | RS.IM-1 | | 3 | | 1.00 | |
| | | RS.IM-2 | | 3 | | 1.00 | |
| Recover (RC) | Recovery Planning (RC.RP) | RC.RP-1 | | 3 | | 1.00 | |
| Recover (RC) | Improvements (RC.IM) | RC.IM-1 | | 3 | | 1.00 | |
| | | RC.IM-2 | | 3 | | 1.00 | |
| Recover (RC) | Communications (RC.CO) | RC.CO-1 | | 3 | | 1.00 | |
| | | RC.CO-2 | | 3 | | 1.00 | |
| | | RC.CO-3 | | 3 | | 1.00 | |
| TOTAL | | | | | | | |

## About Rail Industry Safety and Standards Board

The Rail Industry Safety and Standards Board is a not for profit company limited by guarantee. Wholly owned by its funding members, RISSB is required to apply the whole of its income and assets to achieving the objects listed in its constitution.

RISSB is responsible for the development and management of Standards, Rules, Codes of Practice and Guidelines for the Australian rail industry.

For further information, visit www.rissb.com.au

## RISSB Australian Standards Development Process

The Standards development process is rigorous and transparent.

Authors work with RISSB's Project Managers and Development Groups to ensure that products are acceptable to industry. Standing Committees oversee this work and ensure that proper governance and process is followed. The products are exposed to the public and industry for comment, and validated by an independent validator.

Once agreed by the Development Groups, Standing Committees and Validator, the drafts are passed to the RISSB Board for approval.

The same process is used in developing other RISSB products, although Guidelines are not exposed to the public for comment or validated, given their non-binding nature.

## Standards Development and Accreditation Committee

RISSB is accredited by the Standards Development and Accreditation Committee (SDAC), and all Standards produced by RISSB since 31 July 2007 are published as Australian Standards.

The Standards Development and Accreditation Committee audits RISSB annually to ensure that RISSB's processes are in accordance with SDAC accreditation requirements.

---

## Sales and distribution

Australian Standards developed by RISSB are sold and marketed through SAI Global. For further information, please visit www.saiglobal.com.

Financial members of RISSB are granted access with membership.

RISSB
RAIL INDUSTRY SAFETY AND STANDARDS BOARD

ABN 58 105 001 465

*For information regarding the development of Australian Standards developed by RISSB contact:*

Rail Industry Safety and Standards Board
Suite 4, Level 4, Plaza Offices (*East*)
Terminal Complex, Canberra Airport
ACT 2609 Australia

PO Box 4271, Kingston ACT 2604, Australia

Telephone: 07 3724 0000 (Int. call: +61 7 3724 0000)
Fax: (02) 6270 4516 (Int: +61 2 6270 4516)
email: info@rissb.com.au

*For information regarding the sale and distribution of Australian Standards developed by RISSB contact:*

SAI Global Limited
Phone: 13 12 42
Fax: 1300 65 49 49
Email: sales@saiglobal.com
http://infostore.saiglobal.com/store

ISBN: Enter ISBN.