For queries regarding this document
standards@transport.nsw.gov.au
www.asa.transport.nsw.gov.au

Technical Note - TN 082: 2016

Issued date: 21 December 2016

Subject: Revised reference to risk criteria

This technical note has been issued by the Asset Standards Authority (ASA) to notify the following.

- The risk criteria to be used by the Authorised Engineering Organisations (AEOs) providing engineering services to TfNSW are contained in T MU MD 20002 ST *Risk Criteria for Organisations Providing Engineering Services*, version 1.0.
- 30-ST-164 *TfNSW Enterprise Risk Management (TERM) Standard* provides the risk criteria to be used by TfNSW.
- All references to the TERM standard in this document, where applicable to AEOs, shall read as T MU MD 20002 ST.

Authorisation:

	Technical content prepared by	Checked and approved by	Interdisciplinary coordination checked by	Authorised for release
Signature				
Date				
Name	Richard Adams	Andy Tankard	Andy Tankard	Graham Bradshaw
Position	Manager Safety and Risk Assurance	Principal Manager SQER	Principal Manager SQER	Director Network Standards and Services

For queries regarding this document
standards@transport.nsw.gov.au
www.asa.transport.nsw.gov.au

Technical Note - TN 075: 2016

Issued date: 02 December 2016

Effective date: 02 December 2016

Subject: Amendments to T MU AM 04001 PL *TfNSW Configuration Management Plan*, version 4.0

This technical note is issued by the Asset Standards Authority (ASA) to introduce a number of amendments to T MU AM 04001 PL *TfNSW Configuration Management Plan* version 4.0. The amendments originate from a review of T MU AM 04001 PL conducted with the input of a broad range of stakeholders.

While additional amendments are being considered amendments that are reflective of the continuous growth in the maturity of the configuration management and asset assurance approach of TfNSW are addressed in this technical note.

1. Reference documents

Add the following documents to Section 3.

4SA-SD-404 Terms of Reference - TfNSW Configuration Management and Asset Assurance Committee

TN 073: 2016 Goal structuring notation for configuration management gates

2. Terms and definitions

Add the following terms and definitions to Section 4.

AGP assurance and governance plan

BRS business requirements specification

ISCA initial safety change assessment

RAM reliability, availability and maintainability

SFAIRP so far as is reasonably practicable

SRS system requirements specification

TfNSW Transport Network transport system owned and operated by TfNSW or its operating agencies upon which TfNSW has power to exercise its functions as conferred by the Transport Administration Act or any other Act

3. Scope of the ASA configuration control board

Approval of configuration management plans relating to the delegation of configuration control authority to tier 2 CCBs shall now nominally be the responsibility of the TfNSW CMAAC instead of the ASA CCB.

The ASA CCB may however act as an agent of the TfNSW CMAAC in relation to configuration management process matters including the approval of configuration management plans.

These arrangements amend the configuration management plan approval arrangements described in Section 6.3 of T MU AM 04001 PL and other references to the ASA CCB approval of delegated configuration management plans or delegated configuration management arrangements within the standard.

Replace the final sentence in Section 6.3 –

The ASA CCB holds the authority to approve configuration management plans of organisations seeking authority to make network configuration decisions.

With the following sentence –

The ASA CCB may act as an agent for the CMAAC in relation to making decisions about configuration management processes, including the approval of configuration management plans.

4. TfNSW configuration management and assurance committee

The TfNSW CMAAC is no longer identified as the risk and asset acceptance authority for TfNSW. This means that delegated CCBs will not hold delegated risk acceptance or delegated asset acceptance authority. This change does not affect the practical role of the TfNSW CMAAC or delegated CCBs.

The change represents an evolution in the identification of roles and responsibilities of TfNSW parties. Determinations made by the TfNSW CMAAC represent an outcome that precedes and informs the representative of TfNSW holding responsibility for accepting assets and risks.

This change amends references to the TfNSW CMAAC performing asset acceptance throughout T MU AM 04001 PL. These amendments particularly affect Section 7.1, Section 7.2 and Section 7.3.

Replace the fifth and sixth bullet points in Section 7.1 which read

- asset acceptance authority for network configuration changes
- risk acceptance for configuration changes

With the following bullet point –

- approves configuration management plans relating to the delegation of its configuration control authority

Delete paragraph four and five in Section 7.2 which read

Where the CCB is established within TfNSW, the CCB may also be delegated asset acceptance authority and safety risk acceptance authority for network configuration changes within its delegated scope.

Where the CCB is established external to TfNSW, including CCBs within TfNSW agencies, the CCB may provide asset acceptance and safety risk acceptance but is subject to confirmation by the CMAAC or a delegated TfNSW CCB. Confirmation shall generally be through acceptance of CCB activity reports by the CMAAC or delegated TfNSW CCB.

Delete Section 7.3 Risk acceptance and safety assurance

5. Configuration management plans

Replace all occurrences of ASA CCB with CMAAC in Section 8.

6. Configuration management gates

Figure 2 in Section 12 of T MU AM 04001 PL has been updated to reflect the investment gate naming adopted by TfNSW.

Replace Figure 2 with the following figure.

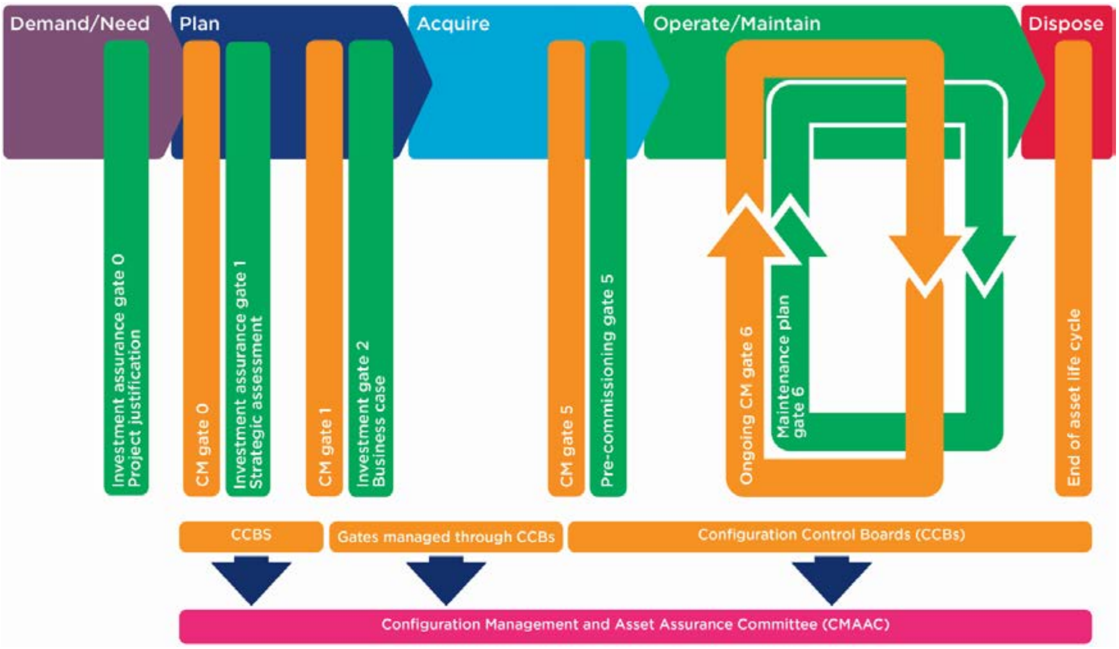


Figure 2 - Assurance gates throughout asset life cycle

7. Minimum requirements for configuration management gates

Minimum requirements for configuration management gates have been revised to improve clarity, to better describe current practice and align with the goal structure diagrams included in TN 073: 2016 *Goal structuring notation for configuration management gates* associated with TS 10753 *Assurance and Governance Plan Requirements*.

Changes have been made to the requirements for gate 0 through to gate 5. No changes have been made to the minimum requirements of gate 6.

7.1. Minimum requirements for gate 0

Replace Section 12.1.1 with the following content.

The configuration change manager (CCM) for a gate 0 submission shall provide the following evidence with the submission:

- initial high level business requirements including an analysis of need and demand
- demonstration of alignment with TfNSW Transport Network strategies and interfacing projects
- high level expectations of the solution from the perspective of the user is understood, such as an operational concept
- relevant stakeholders have been identified and adequately consulted
- appropriately completed safety change assessment; for TfNSW managed projects, an approved initial safety change assessment (ISCA) shall be the acceptable evidence

- safety has been considered in any decisions that affect the final solution
- initial assurance and governance plan (AGP) that demonstrates a systems approach to defining a solution and producing the assurance evidence required for gate 1. The plan shall include demonstration that the following aspects will be addressed:
    - governance and assurance arrangements for how the development of the solution will be progressively assured over the plan phase of the asset life cycle, including at the point when a preferred solution is identified
    - alignment with network strategy
    - whole of life considerations, including operations and maintenance
    - effects on reliability, availability, maintainability and safety of the network
    - risk based decision making
    - development of solutions that are justifiable as safe SFAIRP

7.2. Minimum requirements for gate 1

Replace Section 12.2.1 with the following content.

The CCM for a gate 1 submission shall provide the following evidence with the submission:

- AGP covering the configuration change project through to completion; this should include the approach to configuration management gate submissions particularly proposed CMAAC engagement
- approved business requirements specification (BRS)
- approved system requirements specification (SRS)
- concept of operations
- relevant stakeholder identification and adequate consultation
- risk based decision making in optioneering
- whole-of-life risks have been identified and are being appropriately managed
- appropriately completed safety change assessment, for TfNSW managed projects an approved ISCA shall be acceptable evidence
- human factors considerations as appropriate
- the specified system is one which ensures it is safe so far as is reasonably practicable (SFAIRP)
- independent safety assessment (ISA) report for safety significant changes
- reliability, availability and maintainability (RAM) considerations have been addressed
- whole-of-life costing assessments have been conducted, including operations and maintenance

7.3. Minimum requirements for gate 2

Replace Section 12.3.1 with the following content.

The CCM for a gate 2 submission shall provide the following evidence with the submission:

- compliance to approved assurance and governance arrangements
- approved preliminary design
- proposed solution meets and is traceable to approved requirements presented at gate 1
- hazard log and appropriate management of identified hazards
- whole-of-life risks have been identified and are being appropriately managed
- assessment of safety risk for the given scope to demonstration that it is safe SFAIRP
- Independent Safety Assessor report for significant configuration changes
- relevant stakeholders have been identified and adequately consulted
- RAM considerations have been addressed
- whole of life costing assessments have been conducted to a level appropriate to the significance of the proposed change
- all appropriate technical approvals have been identified and obtained

7.4. Minimum requirements for gate 3

Replace Section 12.4.1 with the following content.

The CCM for a gate 3 submission shall provide the following evidence with the submission:

- compliance to approved assurance and governance arrangements
- solution meets, and is traceable to, approved requirements presented at gate 1
- technical approvals have been identified and obtained, including concessions to ASA requirements or equivalent if required, and final designs have been approved
- hazard log and appropriate management of identified hazards
- whole-of-life risks have been identified and are being appropriately managed
- assessment and documentation of safety risk from a whole of system perspective including residual safety risk has been identified, appropriately managed and agreement obtained from relevant stakeholders such as risk owners and risk control owners
- human factors considerations as appropriate
- Independent Safety Assessor report for safety significant changes
- design safety assurance argument including SFAIRP demonstration from a whole of system perspective

- relevant stakeholders have been identified and adequately consulted
- RAM performance has been considered and assured in the solution
- maintenance requirements have been identified and understood, including that any additional or new maintenance equipment or arrangements have been appropriately addressed
- whole of life costs have been considered and conducted where appropriate
- outstanding issues and assurances are identified with resolution strategies in place
- verification and validation (V&V) strategies during construction are in place
- identification of asset information that should be delivered
- approved for construction (AFC) drawings have been delivered or there is a plan in place for their delivery

7.5. Minimum requirements for gate 4

Replace Section 12.5.1 with the following content.

The CCM for a gate 4 submission shall provide the following evidence with the submission:

- compliance to approved assurance and governance arrangements
- hazard log and appropriate management of identified hazards
- assessment of safety risk for the given scope
- safety assurance argument including SFAIRP demonstration
- relevant stakeholders have been identified and adequately consulted
- technical approvals have been identified and obtained, including concessions to ASA requirements or equivalent if required
- inspection and test plans and strategy to a level appropriate to the significance of the proposed change
- outstanding issues and assurances are identified with resolution strategies in place

7.6. Minimum requirements for gate 5

Replace Section 12.6.1 with the following content.

The CCM for a gate 5 submission shall provide the following evidence with the submission:

- compliance to approved assurance and governance arrangements
- hazard log and appropriate management of identified hazards
- operational and maintenance readiness arrangements have been appropriately managed
- assessment of safety risk for the given scope, generally a safety assurance report (SAR)

- asset and operational safety argument demonstrating that the asset ensures safety SFAIRP in its intended operational context
- ISA, that includes operational safety, for safety significant changes
- risk register including identification of residual risks
- suitable and sufficient reliability, availability and maintainability performance has been assured
- relevant stakeholders have been identified and adequately consulted
- demonstration that solution meets approved requirements
- RAM considered as appropriate in the delivered solution
- whole of life cost assessments have been prepared for handover where appropriate
- technical approvals have been identified and obtained, including concessions to ASA requirements or equivalent if required
- identification of asset information has been delivered and that there is a schedule for delivery of outstanding asset information
- where the submission relates to a handover to a service provider, agreement from the manager of the relevant operate and maintain contract that the applicable operator and maintainer is ready to receive the asset
- outstanding issues and assurances are identified with resolution strategies in place

8. Clarification of application of T MU AM 04001 PL to specific circumstances

To facilitate the application of T MU AM 04001 PL, additional clarifications have been provided in this technical note. The clarifications cover circumstances that commonly arise in the course of applying T MU AM 04001 PL.

8.1. Minimum requirements for gate 6

Add the following new sections after 12.7.1

12.8. Tailoring the application of configuration management gates

The configuration management gates described in this technical note and T MU AM 04001 PL are standard requirements applicable to configuration changes to TfNSW transport infrastructure. The nature and risk associated with configuration changes can however vary substantially; thus it may be appropriate for arrangements applicable to specific situations to vary from the standard requirements either to improve efficiency or provide adequate governance. Variations shall be documented and shall be approved by the CMAAC or appropriately delegated body. Variations to the application of configuration management gates, that are to be adopted as standard practice, shall generally be described within the applicable configuration management plan or otherwise documented, approved and associated with the applicable configuration management plan. Variations for specific cases may be documented as decisions of the CMAAC or delegated body.

Variations to the application of gates shall meet the intent of this document. Arrangements other than those described in this document should be mapped against the configuration management gates described in this document.

12.9. Application of configuration management gates to maintenance

Maintainers of TfNSW transport assets are generally expected to develop a configuration management plan, including arrangements for the application of configuration management gates and have it accepted by the CMAAC or delegate. This may include a tailored approach as clarified in Section 12.8 of this technical note where appropriate.

As maintenance activities can vary greatly in scale, complexity and risk, the application of gates to maintenance configuration changes may require defining and adjusting based on these factors. Maintenance activities resulting in moderate or minor configuration changes performed as part of a maintenance contract may not require the application of gate 0 or gate 1. This can occur where the need for the configuration change or the methodology for determining the need for the configuration change has been identified and documented in asset maintenance plans and annual works plans or equivalent. Such plans are reviewed by TfNSW and support a gate 6 submission by the responsible TfNSW business unit to the CMAAC.

12.10. Application of configuration management gates to decommissioning

Decommissioning of TfNSW transport assets or assets that integrate with TfNSW transport assets is a configuration change. Decommissioning of TfNSW transport assets will often occur as part of a broader project that introduces other new or altered assets and shall be managed through gates as part of that work.

Although decommissioning of assets can include the complete removal of assets, interfaces may need to be managed and asset information updated. In some cases a tailored approach as clarified in Section 12.8 of this technical note may be appropriate.

12.11. Application of configuration management gates to third party work

Configuration management processes shall be applied to changes initiated and predominantly managed by third parties. Third party work includes work on third party assets interfacing with TfNSW transport infrastructure or work initiated and managed by a third party resulting in new or changed TfNSW transport assets.

Third party configuration changes are generally initiated, designed and delivered by a third party. The configuration change may also predominantly impact assets other than those owned or controlled by TfNSW and as such appropriate requirements for configuration management gates can vary from the standard arrangements depending on the nature of the change. The risk and impact to TfNSW shall be considered in any tailored approach to the application of configuration management gates to third party work. Typically, gate 3 and gate 5 or equivalent would apply as a minimum as there is a need for TfNSW to be assured prior to the implementation of the final solution and to be assured that the implementation is as planned.

As third party changes occur on TfNSW transport infrastructure typically managed by a TfNSW contracted maintainer, the contracted maintainer is generally responsible for documenting and managing appropriate risk based configuration change processes. Third party work that introduces a significant configuration change to TfNSW is expected to have appropriate engagement with the CMAAC in a similar manner to other significant configuration changes.

The CCM for third party work is typically the person within TfNSW or transport agency responsible for managing the interface to the transport network.

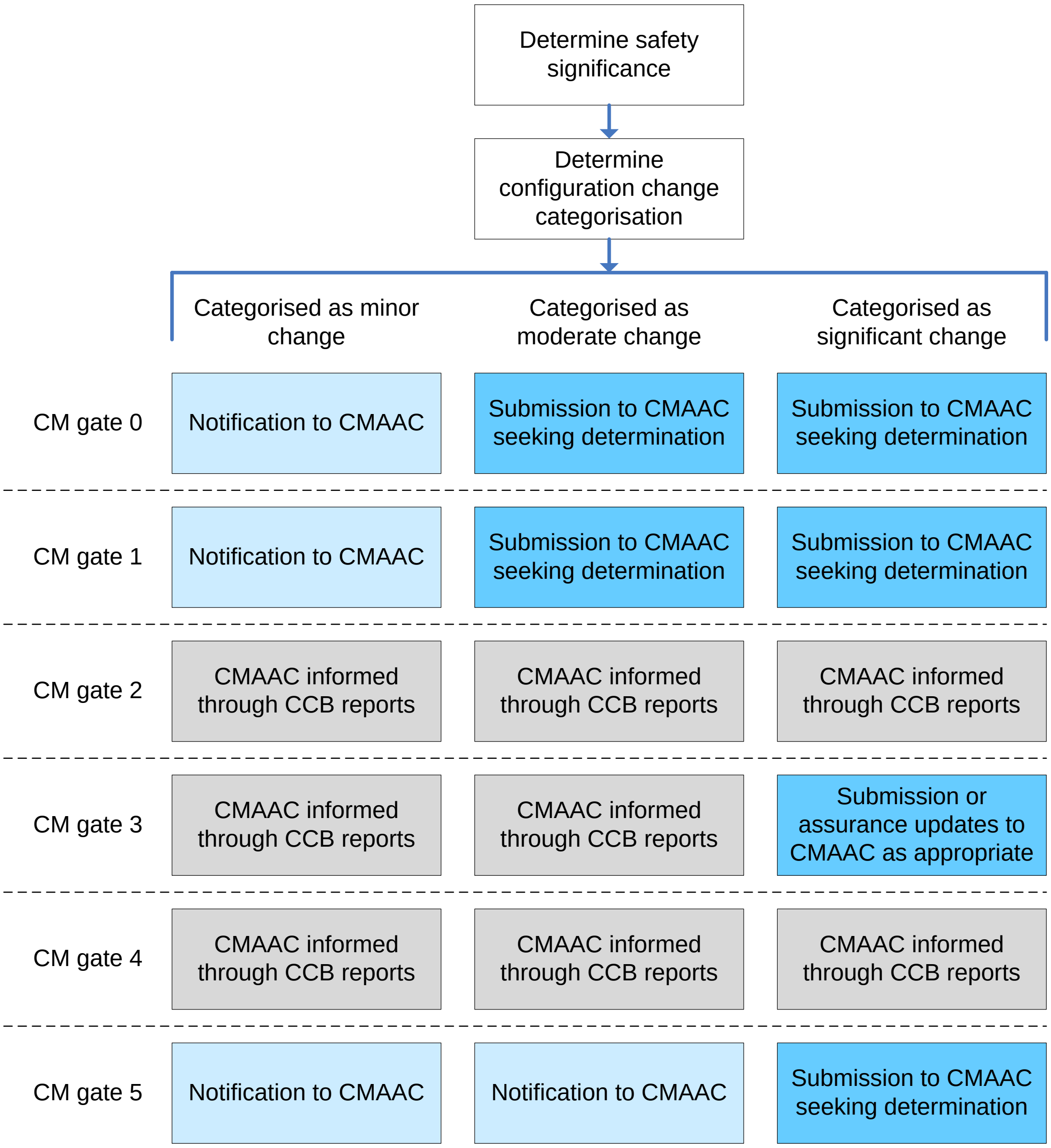
9. Configuration change significance and CMAAC engagement

Amendments and clarifications relating to the presentation of submissions to the TfNSW CMAAC are made through this technical note. The amendments relate predominantly to the change in the increased focus by CMAAC on gate 3, reduced focus by CMAAC on gate 5 and the removal of the requirement that all gate 5 submissions be presented to CMAAC for determination.

Replace Section 13.5 with the following content.

The level of engagement required with the CMAAC is largely determined by the categorisation of a configuration change. Variations to the engagement with the CMAAC may continue to occur where there is a CMAAC approved AGP or approved configuration management plan documenting the alternate approach or specific agreement from the CMAAC or the ASA.

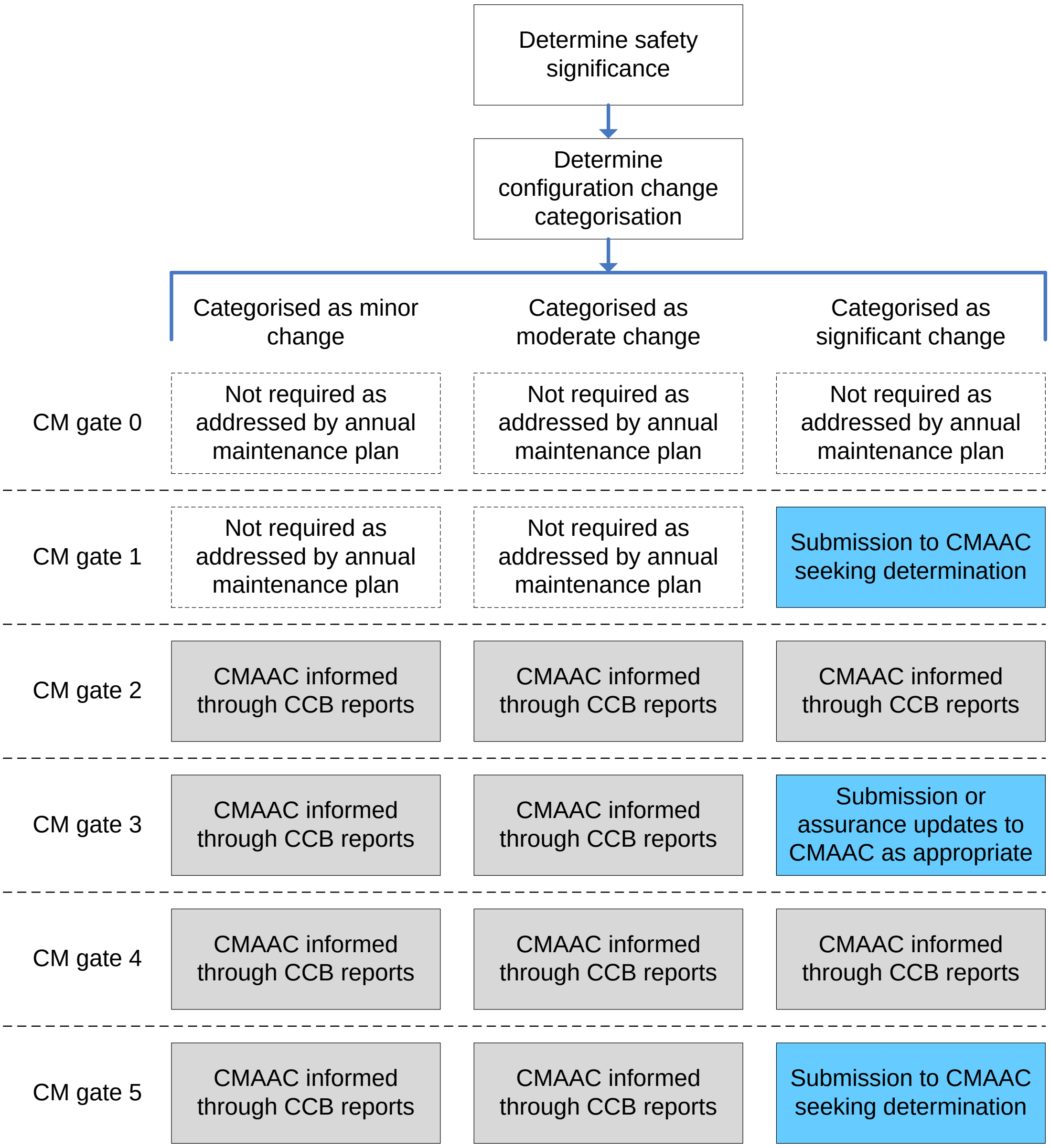
The normal approach for engaging with the CMAAC for a configuration change that is not part of an asset maintenance plan accepted by the CMAAC as part of a configuration management gate 6 submission is shown in Figure 3.1. Typically such configuration change projects are classified by TfNSW as capital expenditure.


Determine safety significance
Determine configuration change categorisation

	Categorised as minor change	Categorised as moderate change	Categorised as significant change
CM gate 0	Notification to CMAAC	Submission to CMAAC seeking determination	Submission to CMAAC seeking determination
CM gate 1	Notification to CMAAC	Submission to CMAAC seeking determination	Submission to CMAAC seeking determination
CM gate 2	CMAAC informed through CCB reports	CMAAC informed through CCB reports	CMAAC informed through CCB reports
CM gate 3	CMAAC informed through CCB reports	CMAAC informed through CCB reports	Submission or assurance updates to CMAAC as appropriate
CM gate 4	CMAAC informed through CCB reports	CMAAC informed through CCB reports	CMAAC informed through CCB reports
CM gate 5	Notification to CMAAC	Notification to CMAAC	Submission to CMAAC seeking determination

Figure 3.1 – Normal approach to engaging with CMAAC for configuration changes not included within an approved asset maintenance plan

The normal approach for engaging with the CMAAC for configuration changes that are included within an asset maintenance plan that has been accepted by CMAAC at configuration management gate 6 is shown in Figure 3.2.



Determine safety significance

Determine configuration change categorisation

	Categorised as minor change	Categorised as moderate change	Categorised as significant change
CM gate 0	Not required as addressed by annual maintenance plan	Not required as addressed by annual maintenance plan	Not required as addressed by annual maintenance plan
CM gate 1	Not required as addressed by annual maintenance plan	Not required as addressed by annual maintenance plan	Submission to CMAAC seeking determination
CM gate 2	CMAAC informed through CCB reports	CMAAC informed through CCB reports	CMAAC informed through CCB reports
CM gate 3	CMAAC informed through CCB reports	CMAAC informed through CCB reports	Submission or assurance updates to CMAAC as appropriate
CM gate 4	CMAAC informed through CCB reports	CMAAC informed through CCB reports	CMAAC informed through CCB reports
CM gate 5	CMAAC informed through CCB reports	CMAAC informed through CCB reports	Submission to CMAAC seeking determination

Figure 3.2 - Normal approach to engaging with CMAAC for configuration changes included within an approved asset maintenance plan

Submissions to the CMAAC result in an explicit determination made by the CMAAC. Determinations are made in accordance with 4SA-SD-404 *Terms of Reference - TfNSW Configuration Management and Asset Assurance Committee*. Submissions to the CMAAC are expected to be endorsed by a delegated CCB prior to being presented to the CMAAC if an appropriate CCB exists.

Notifications presented to the CMAAC are tabled to the CMAAC members for noting and do not require an explicit determination from the CMAAC, though the CMAAC may still make a specific determination or raise an action if they deem appropriate. Notifications are expected to be accepted by a delegated CCB prior to being presented to the CMAAC where an appropriate delegated CCB exists.

Authorisation:

	Technical content prepared by	Checked and approved by	Interdisciplinary coordination checked by	Authorised for release
Signature				
Date				
Name	Garry Thong	Garry Thong	Toby Horstead	Graham Bradshaw
Position	Manager Asset Configuration Systems	Manager Asset Configuration Systems	Principal Manager Network and Asset Strategy	Director Network Standards and Services

T MU AM 04001 PL

Plan

TfNSW Configuration Management Plan

Version 4.0

Issued date: 14 August 2015

Important Warning

This document is one of a set of standards developed solely and specifically for use on Transport Assets (as defined in the Asset Standards Authority Charter). It is not suitable for any other purpose.

You must not use or adapt it or rely upon it in any way unless you are authorised in writing to do so by a relevant NSW Government agency. If this document forms part of a contract with, or is a condition of approval by a NSW Government agency, use of the document is subject to the terms of the contract or approval.

This document is uncontrolled when printed or downloaded. Users should exercise their own skill and care in the use of the document.

This document may not be current. Current standards may be accessed from the Asset Standards Authority website at www.asa.transport.nsw.gov.au.

Standard governance

Owner: Manager Asset Configuration Systems, Asset Standards Authority

Authoriser: Principal Manager Network and Asset Strategy, Asset Standards Authority

Approver: Director, Asset Standards Authority on behalf of the ASA Configuration Control Board

Document history

Version	Summary of Changes
1.0	First issue
2.0	Minor update to configuration management authority delegation structure figure
3.0	Minor update to asset life cycle diagram and clarifications
4.0	Minor update to remove rail focused statements, clarify a term, and update the asset life cycle diagram

For queries regarding this document,
please email the ASA at
standards@transport.nsw.gov.au
or visit www.asa.transport.nsw.gov.au

Preface

The Asset Standards Authority (ASA) is an independent unit within Transport for NSW (TfNSW) and is the network design and standards authority for defined NSW transport assets.

The ASA is responsible for developing engineering governance frameworks to support industry delivery in the assurance of design, safety, integrity, construction, and commissioning of transport assets for the whole asset life cycle. In order to achieve this, the ASA effectively discharges obligations as the authority for various technical, process, and planning matters across the asset life cycle.

The ASA collaborates with industry using stakeholder engagement activities to assist in achieving its mission. These activities help align the ASA to broader government expectations of making it clearer, simpler, and more attractive to do business within the NSW transport industry, allowing the supply chain to deliver safe, efficient, and competent transport services.

The ASA develops, maintains, controls, and publishes a suite of standards and other documentation for transport assets of TfNSW. Further, the ASA ensures that these standards are performance-based to create opportunities for innovation and improve access to a broader competitive supply chain.

The ASA is the owner of the configuration management framework for TfNSW and sets the standards for configuration management of New South Wales transport assets.

This plan has been prepared and reviewed by the ASA configuration control board and approved by the Director, Asset Standards Authority. Requirements and standard processes for the application of configuration management and associated assurance of assets throughout its asset life cycle of NSW transport assets are established by this plan.

This document is the fourth issue. The changes compared to the previous version include removing rail focused statements, additional clarification of the term 'product configuration information' in the terms and definitions and an update of the asset life cycle diagram to include terms that are consistent with other configuration documents published by the ASA.

The requirements of this document form part of the Asset Standards Authority configuration management framework and are consistent with the TfNSW CP14005 *Transport Asset Management Policy*.

Table of contents

1. Introduction

This *TfNSW Configuration Management Plan* sets out Transport for New South Wales (TfNSW) arrangements for managing the configuration of its transport assets and the acceptance and assurance of assets.

Arrangements described in this plan define the governance structure for the management of configuration changes. The arrangements are to assure that configuration changes are appropriately managed to meet the defined technical requirements throughout an asset's life and are safe so far as is reasonably practicable (SFAIRP). The governance structure and configuration change acceptance arrangements described in this plan integrate with the TS 20001: 2013 *System Safety Standard for New and Altered Assets* and are consistent with the intent of TfNSW's CP14005 *Transport Asset Management Policy* and 50-ST-162/3.0 *Asset Lifecycle Safety Management Standards*.

2. Purpose

This *TfNSW Configuration Management Plan* operates as the highest level configuration management plan for TfNSW and does so in conjunction with the TS 20001: 2013 *System Safety Standard for New or Altered Assets*. This document includes the establishment of a standard framework to facilitate coordination and communication between TfNSW, TfNSW agencies and Authorised Engineering Organisations (AEOs) that perform configuration management and asset assurance activities.

2.1. Scope

This document addresses how configuration management principles are applied to the requirement of TfNSW to manage the configuration of its transport assets. The scope of this document is limited to network configuration management. This includes the activities, systems and documentation that form part of the integration of assets with the TfNSW transport network.

This plan operates in conjunction with TS 20001: 2013.

2.2. Application

This *TfNSW Configuration Management Plan* applies to TfNSW, TfNSW agencies and contracted entities that are responsible for the following:

- TfNSW transport infrastructure or fleet
- assets, operations and systems that interface with TfNSW transport infrastructure or fleet
- documents that define TfNSW transport asset configuration

3. Reference documents

The following documents are cited in the text. For dated references, only the cited edition applies. For undated references, the latest edition of the referenced document applies.

Australian standards

AS ISO 10007-2003 – Quality management systems – Guidelines for configuration management

Transport for NSW standards

30-ST-164 TfNSW Enterprise Risk Management (TERM) Standard (available on request from standards@asa.transport.nsw.gov.au)

50-ST-162/3.0 Asset Lifecycle Safety Management Standard (available on request from standards@asa.transport.nsw.gov.au)

TS 10753: 2014 – Assurance and Governance Plan Requirements

TS 20001: 2013 – System Safety Standard for New or Altered Assets

Other reference documents

Asset Standards Authority Charter

CP14005 Transport Asset Management Policy (available on request from standards@asa.transport.nsw.gov.au)

20-FT-388 Initial Safety Change Assessment (available on request from standards@asa.transport.nsw.gov.au)

4. Terms and definitions

The following terms and definitions apply in this document:

AEO Authorised Engineering Organisation

the ASA the Asset Standards Authority

asset acceptance the acceptance of a new or altered asset into the transport network for operation and maintenance by a contracted body

business unit means a part of an organisation with a defined scope or responsibility

CCB configuration control board

change control activities for control of the product

CMAAC Configuration Management and Asset Assurance Committee (TfNSW)

configuration interrelated functional and physical characteristics of a product defined in product configuration information

configuration audit an examination to determine whether a configuration item conforms to its approved configuration baseline

configuration baseline an approved product configuration that establishes the characteristics of a product at a point in time that serves as reference for activities throughout the life cycle of the product

configuration change manager the person who has primary responsibility for a configuration change

configuration change request a formal request to add or change a TfNSW transport asset that is subject to configuration control

configuration control board a person or a group of persons assigned responsibility and authority to make decisions on the configuration

configuration documents product configuration information and its supporting medium

configuration identification activities comprising determination of the product structures, selection of configuration items, documenting the configuration item's physical and functional characteristics including interfaces and subsequent changes, and allocating identification characters or numbers to the configuration items and their documents

configuration information custodian a person who has responsibility for managing configuration information

configuration information system custodian a person who is responsible for managing a system that contains product configuration information. The system is the repository and processes, procedures and tools for receiving, maintaining and making available the product configuration information

configuration item an entity within a configuration that satisfies an end use function

configuration management coordinated activities to direct and control configuration

configuration status accounting formalised recording and reporting of product configuration information, the status of proposed changes, and the status of the implementation of approved changes

network configuration the configuration of transport assets viewed as a system that is for achieving the business objectives of TfNSW and is composed of discrete configuration items identified at a level commonly identified by TfNSW

product configuration information requirements for product design, realisation, verification, operation and support. May also be referred to as asset information or configuration information

TfNSW Transport for New South Wales

transport assets assets associated with the maintenance and operation of the transport network

5. Configuration management responsibilities of TfNSW

TfNSW transport asset configuration responsibilities encompass the following aspects:

- the configuration and proposed changes to the configuration of its transport infrastructure, fleet including the addition of new assets
- documentation defining configuration of its transport infrastructure and fleet, including engineering standards
- matters arising from the interface of its transport infrastructure and fleet with TfNSW transport operations and other associated systems
- matters arising from the interface of its transport infrastructure and fleet with the assets and operations of any other entity
- hardware and software used in its configuration management systems, particularly in the production, collection and storage of configuration data and documents, and in change control procedures

Configuration management and its associated processes operate throughout the full life cycle of its assets including project initiation and disposal.

6. Governance arrangements

Governance arrangements for configuration management define the arrangements and parties with the authority to make decisions about the configuration of the network and asset acceptance.

6.1. Process ownership and decision making

Ultimate accountability for the configuration of TfNSW transport assets rests with the Secretary of TfNSW. The Secretary TfNSW discharges accountability for configuration management by authorising the Asset Standards Authority to set the framework for configuration management via the ASA Charter.

The configuration management framework set by the ASA includes the following two governance bodies that are considered Tier 1 configuration control boards:

- TfNSW Configuration Management and Asset Assurance Committee (CMAAC) established within TfNSW that is the network configuration change and asset acceptance body and the asset acceptance body for TfNSW.
- A configuration control board (CCB) established within the ASA. The ASA CCB has authority to set configuration management requirements for TfNSW and has configuration

change control authority over its configuration items. The ASA's configuration items are the requirements set by the ASA applicable to other parties.

6.1.1. Tier structure of delegated CCBs

Configuration control boards may be established to facilitate the configuration management, assurance and staged asset acceptance of transport assets by receiving delegated authority over a defined scope of assets or stage of an asset life cycle. Such configuration control boards reside directly below the CMAAC in hierarchy and are considered Tier 2 configuration control boards.

Additional configuration control boards or delegated entities may also be established or defined that reside below the Tier 2 configuration control boards. Generally, Tier 2 CCBs will be established within TfNSW or an operator maintainer.

Contracted parties delivering configuration changes and who establish their own CCBs for making network configuration change decisions shall operate within the hierarchy in Figure 1 and shall generally operate as Tier 3 CCBs. Tier 3 CCBs shall operate under configuration management arrangements accepted by the Tier 2 CCB that delegates its authority to the Tier 3 CCB.

Figure 1 provides a representation of the delegation of authority for configuration management within TfNSW.

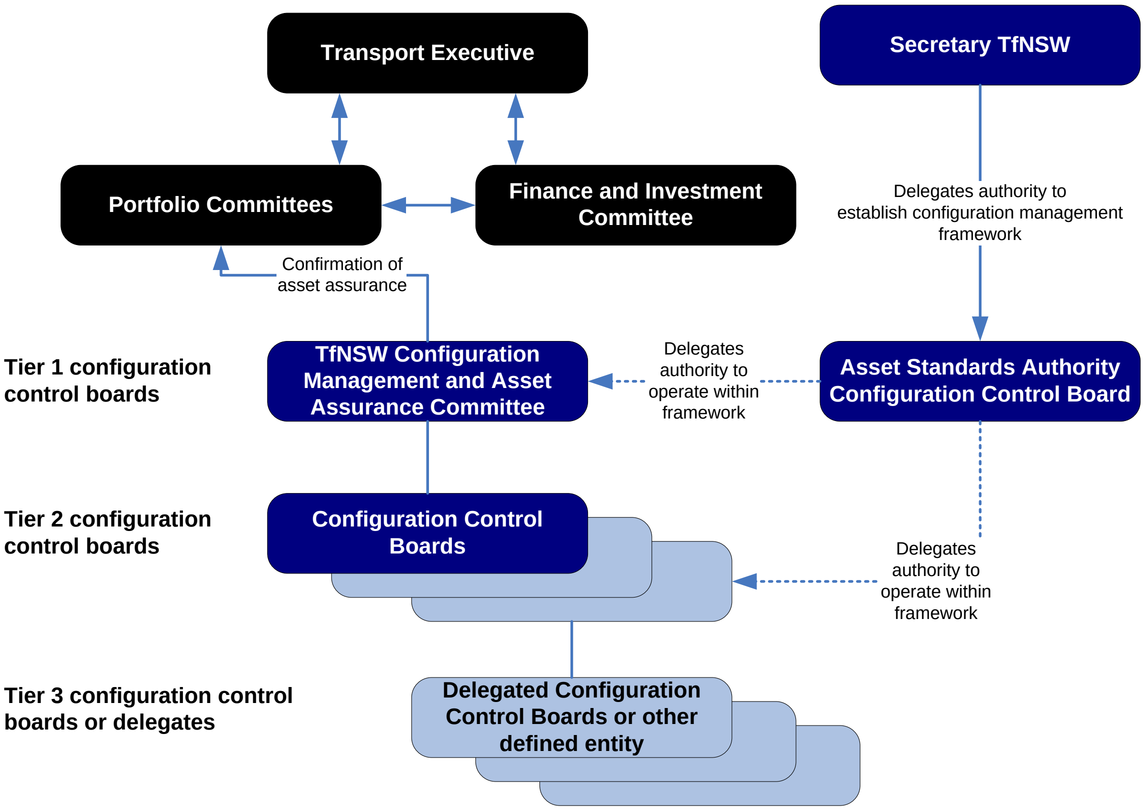

Transport Executive
Secretary TfNSW
Portfolio Committees
Finance and Investment Committee
Delegates authority to establish configuration management framework
Confirmation of asset assurance
Tier 1 configuration control boards
TfNSW Configuration Management and Asset Assurance Committee
Delegates authority to operate within framework
Asset Standards Authority Configuration Control Board
Tier 2 configuration control boards
Configuration Control Boards
Delegates authority to operate within framework
Tier 3 configuration control boards or delegates
Delegated Configuration Control Boards or other defined entity

Figure 1 - Configuration management authority delegation structure

6.2. Configuration information ownership

The Secretary TfNSW, through the ASA charter, has defined the ASA as the owner of TfNSW configuration information on behalf of TfNSW.

Configuration information includes the following information sets:

- physical characteristics
- functional characteristics
- performance history
- maintenance requirements
- operational requirements
- documentation that assures the designed configuration such as design calculations and hazard logs

As the owner of the configuration information, the ASA shall define the requirements for the management of the information. Where specific requirements have not been defined by the ASA, then existing arrangements shall apply until superseded by ASA requirements.

Systems holding the configuration information owned by the ASA do not have to be owned by the ASA but need to meet any applicable requirements of the ASA.

6.3. Scope of the ASA configuration control board

The ASA has established a CCB to manage its configuration items. Configuration items of the ASA are the requirements, or any other content of a similar nature owned by the ASA and that are applicable external to the ASA. This includes standards and Authorised Engineering Organisation (AEO) requirements. It may include published guidance and other documents that influence the technical or asset management activities of parties external to the ASA. The ASA CCB holds the authority to approve configuration management plans of organisations seeking authority to make network configuration decisions.

6.4. Delegation of network configuration control and asset assurance authority

Organisations, including AEOs and business units of TfNSW may be delegated responsibility and authority to make decisions about network configuration changes on TfNSW transport assets on behalf of the CMAAC. Authority is to be exercised within a framework and scope approved by the ASA CCB. The delegation of authority to make decisions on network configuration changes includes the authority and responsibility for asset acceptance.

To receive delegated configuration control authority, an organisation shall have a configuration management plan approved by the ASA CCB, as the ASA is the owner to the TfNSW configuration management framework. The plan shall describe the configuration management arrangements, asset assurance, and asset acceptance arrangements that the organisation will apply. The configuration management plan shall clearly identify how delegated authority will be exercised and how assurances will be provided to the ASA and the CMAAC that configuration decisions have been properly managed.

Such configuration management plans shall also be approved though through the organisation's own arrangements.

When the ASA CCB considers the approval of a configuration management plan, the risk and appropriateness of the delegation arrangements will be reviewed. Proposed configuration management plans should reflect this requirement.

Approval of an organisation's configuration management plan by the ASA CCB only covers aspects of the plan addressing network configuration change and asset assurance in relation to TfNSW transport assets and related interfaces.

6.4.1. Relationship of delegation of authority to AEO status

Delegated authority for network configuration control, asset assurance and asset acceptance is not automatically provided to AEOs. AEOs are required to demonstrate the capability to perform configuration management activities applicable to the engineering services that they are authorised to provide.

Delegated authority for network configuration control and asset assurance is only required where the AEO has been engaged as the party responsible for network configuration and asset assurance on behalf of TfNSW.

6.4.2. Reporting to the ASA and the CMAAC

Organisations that have delegated authority for making network configuration decisions shall provide reports to the ASA demonstrating the appropriate exercise of that authority. The ASA shall consolidate and distribute reports to the CMAAC as appropriate or as requested by the CMAAC. Reporting shall be documented within the organisation's configuration management plan.

Regular reports shall provide a summary and listing of the following aspects:

- the status of configuration change requests
- any configuration changes that occurred without configuration change approval
- configuration audits performed
- forecasts of future configuration change requests
- any other configuration management matters that the ASA should be aware of

Reports shall be provided monthly unless other arrangements are agreed with the ASA.

Exercise of configuration control authority is subject to surveillance audits by the ASA.

7. Configuration management responsibilities

Configuration management responsibilities are allocated through this plan to various parties that participate in the asset life cycle. The responsibilities are established in this plan but may be tailored though arrangements defined in approved lower level configuration management plans.

7.1. TfNSW configuration management and asset assurance committee

The CMAAC is the top level configuration control board (CCB) responsible for network configuration decisions about existing or proposed TfNSW transport assets.

The role of the CMAAC is to oversee the application of network configuration management and asset assurance, including safety risk management on TfNSW transport assets. The CMAAC achieves this by holding the acceptance authority for network configuration changes and asset acceptance. In exercising these authorities, the CMAAC seeks evidence that appropriate assurance activities have been conducted on the following aspects:

- development of proposed transport asset configuration changes
- delivery of the transport asset configuration changes
- maintenance of approved transport asset configuration

The CMAAC performs the following roles:

- determining authority on configuration management issues that affect TfNSW transport assets
- asset acceptance authority for network configuration changes
- risk acceptance for configuration changes

CMAAC responsibilities include the following:

- providing direction, guidance, recommendations and oversight for the development and implementation of configuration management, asset assurance and asset acceptance
- reviewing and granting configuration change acceptance if satisfied that evidence of assurance associated with a configuration change request is adequate
- facilitating the resolution of issues not resolved by configuration change managers, stakeholders or other CCBs
- delegating configuration management responsibility and authority at its discretion

In reviewing configuration change requests the CMAAC shall seek assurance, where appropriate, that the following have been adequately addressed:

- business and system requirements have been developed and approved
- stakeholders have been identified and consulted
- safety assessments, reports and other assurance activities have been conducted and have been subject to appropriate review, verification or independent assessment
- technical approvals have been obtained
- configuration information has been produced, assured and provided to TfNSW or its representative
- preceding configuration change management approvals have been obtained
- operational and maintenance arrangements have been resolved
- independent safety assessment has been performed for significant changes

7.2. Configuration control board responsibilities

CCBs that have authority for network configuration change control shall make decisions in the interest of TfNSW. Where such CCBs are established outside of either TfNSW or a TfNSW agency, the board shall include representation from TfNSW or otherwise demonstrate that the interests of TfNSW are addressed.

The role of a CCB is to provide management control over TfNSW transport configuration matters that fall within the areas of responsibility of each CCB.

CCBs are determining authorities on configuration management issues affecting TfNSW transport assets within the delegated scope of that CCB.

Where the CCB is established within TfNSW, the CCB may also be delegated asset acceptance authority and safety risk acceptance authority for network configuration changes within its delegated scope.

Where the CCB is established external to TfNSW, including CCBs within TfNSW agencies, the CCB may provide asset acceptance and safety risk acceptance but is subject to confirmation by the CMAAC or a delegated TfNSW CCB. Confirmation shall generally be through acceptance of CCB activity reports by the CMAAC or delegated TfNSW CCB.

CCB responsibilities include the following:

- facilitate the resolution of issues not resolved by configuration change managers and stakeholders
- ensure documented systems are in place to allow it to conduct its business and exercise its authority effectively and efficiently

- provide traceability and assurance to the ASA and TfNSW that all configuration changes within the responsibility of the CCB have been properly managed and decisions have been in the interest of TfNSW
- appropriate whole of life solution has been justified

7.2.1. The ASA configuration control board

The Director Asset Standards Authority has established a CCB to make configuration decisions for the configuration items for which the ASA is responsible.

7.3. Risk acceptance and safety assurance

As the asset acceptance body for TfNSW, the CMAAC shall review the evidence of asset assurances, including safety assurance that is provided by a project when a configuration change request is submitted to the CMAAC. Risk acceptance by the CMAAC will only be required at specific gates of the project. The requirements of safety risk acceptance and safety assurance are specified in TS 20001: 2013 *System Safety Standard for New or Altered Assets*.

Unless otherwise specified, when network configuration control authority is delegated from the CMAAC to a TfNSW CCB, the corresponding risk acceptance responsibilities are also delegated.

7.4. Responsibilities of contracted AEOs that deliver new or altered assets

Contracted AEOs with primary responsibility for the delivery of new or altered transport assets shall establish at least one CCB; provide at least one configuration management plan that defines the governance structure that the AEO's CCB operates under; and, have an assurance and governance plan that covers its configuration changes. Primary responsibility in this context typically applies to occasions where the contracted AEO does not operate under the scope of another Tier 2 CCB. The AEO's configuration management plans shall comply with this *TfNSW Configuration Management Plan* and TS 20001: 2013.

7.5. Responsibilities of contracted AEOs that perform maintenance

Contracted AEOs that have primary responsibility for the maintenance of TfNSW transport assets are also responsible for maintaining the configuration of those assets and maintaining the accuracy of the configuration information describing those assets.

Such AEOs shall develop at least one configuration management plan that complies with this *TfNSW Configuration Management Plan* and TS 20001: 2013.

An AEO performing maintenance shall establish at least one CCB with configuration control authority for the scope of the changes being delivered as part of its maintenance activities.

7.6. Configuration change managers

The person who has primary responsibility for managing a configuration change is known as the configuration change manager. The project manager of a configuration change is generally the configuration change manager.

A configuration change manager may engage other persons to carry out required tasks, but is ultimately responsible for ensuring due process. Primary responsibility for a configuration change may vary as the change process progresses.

The role of the configuration change manager is to ensure that the asset is designed and implemented to be fit for purpose, safe, reliable, maintainable and optimised for whole of life costs.

The following are general responsibilities of configuration change managers:

- determine the level of significance of the configuration change
- register and manage the progress of configuration change requests
- follow due process and perform whatever activities are necessary to identify and address stakeholder issues and obtain primary stakeholder signoff on configuration change requests
- maintain a documented audit trail of the change
- provide configuration information in the format required for updating configuration information systems when a change is implemented
- meet requirements for finalising a configuration change request after the configuration change has been fully implemented and all information systems updated
- obtain configuration change approval before allowing the change to occur
- meet any additional requirements applied by the CCB they are seeking approval from

7.7. Configuration change stakeholders

The following are the tasks of stakeholders:

- review and determine whether a proposed change has any adverse effects on the business unit's responsibilities
- make a decision or recommendation on the acceptability to the business unit of a proposed change

- cooperate with configuration change managers to identify and resolve issues and adverse effects

7.7.1. Primary stakeholders

Primary stakeholders hold authority to make decisions on behalf of the organisation or business unit they represent. The consent of the primary stakeholder represents agreement that the organisation's or business unit's requirements, comments, or impacts have been satisfactorily addressed.

The role of primary stakeholder and the means of identifying primary stakeholders should be applied as appropriate for each organisation operating to this plan.

7.7.2. Stakeholder nomination

Contracted AEOs and senior managers in TfNSW that could be affected by the configuration of current or proposed TfNSW transport assets or interfacing operations, shall nominate adequate stakeholders to ensure that effects of proposed changes on their business units are identified and adequately assessed.

Nominated stakeholders shall generally meet the following criteria:

- all functional areas potentially affected by changes should be represented
- stakeholders should be senior officers in a functional area
- only one stakeholder per functional area

7.7.3. Stakeholder consent

Primary stakeholder consent indicates that stakeholder consultation for their business unit or organisation has been adequate.

Primary stakeholder consent from affected business units is a requirement for CCB approval of a configuration change request, unless otherwise determined by the responsible CCB or otherwise defined within an approved configuration management plan.

7.7.4. Technical approval

Configuration management stakeholder consent does not constitute technical approval, even if the stakeholder has the authority to provide such approval. Technical approval is a separate approval obtained where required.

8. Configuration management plans

Business units within TfNSW that have input to the management or establishment of the configuration of the TfNSW transport network, shall operate under this configuration management plan but may produce subsequent configuration management plans compliant to this plan. Where a business unit of TfNSW establishes a CCB, it may operate under this configuration management plan, or under its own configuration management plans if approved by the ASA CCB.

Contracted AEOs that have been engaged as the primary party responsible for managing the network integration of new or altered TfNSW transport assets, or are the primary party responsible for maintaining the configuration of TfNSW transport assets, shall have a configuration management plan that has been approved by the ASA CCB. AEOs in this category shall establish a Tier 2 CCB below the CMAAC.

Contracted AEOs with responsibility for network integration but operating within the remit of an existing Tier 2 CCB do not require a configuration management plan that has been approved by the ASA CCB, but shall operate under the governance arrangements established by the respective Tier 2 CCB.

9. System requirements of organisations with responsibility for network configuration control

Organisations with primary responsibility for network configuration management shall have a configuration management system to manage the configuration of those TfNSW transport assets they are in control of. The system is to consist of plans, procedures, tools, and other elements necessary to fulfil satisfactorily their responsibilities of maintaining configuration change or maintaining the configuration of assets and associated configuration information. The plans shall describe arrangements for the progressive assurance during the introduction of new and altered assets and the continuous assurance of existing assets.

9.1. Performance requirements

Configuration management systems developed and implemented by organisations with delegated network configuration control authority shall achieve the following requirements:

- comply with this *TfNSW Configuration Management Plan*
- comply with AS ISO 10007 *Quality management systems -- Guidelines for configuration management*
- comply with the requirements of the TS 20001: 2013
- assure TfNSW, through evidence, that the configuration of current or proposed TfNSW transport assets under the control of the AEO is managed appropriately
- assure TfNSW that roles and responsibilities for configuration management within the AEO are clearly identified and documented

- assure TfNSW that configuration change stakeholders are identified and appropriately consulted
- assure TfNSW that appropriate configuration change stakeholders in the organisation participate in consultation when requested by a configuration change manager internal or external to the organisation
- assure TfNSW of due process prior to any configuration change
- assure the ASA that the configuration information of TfNSW transport assets under its control is accurate and appropriate for the ongoing management of the assets
- assure TfNSW that issues that affect or may affect the integrity of TfNSW transport assets or the configuration information that describes it is reported to TfNSW and other responsible parties where applicable

9.2. Minimum requirements of system

Configuration management systems developed and implemented by organisations with delegated network configuration control authority shall, at minimum, include the following elements:

- a configuration management plan that is consistent with both this *TfNSW Configuration Management Plan* and AS ISO 10007
- documented roles and responsibilities
- defined or identified configuration management processes and requirements that support the assurance that assets are safe SFAIRP (so far as is reasonably practicable) and whole of life aspects are appropriately managed
- tools and templates to be used for managing configuration
- a description of how stakeholder input is determined, obtained, recorded and addressed
- identified configuration management authorities and responsibilities delegated by TfNSW and descriptions of how those responsibilities and authorities are managed
- a surveillance framework that demonstrates that there is adequate control of configuration management and that configuration information accurately reflects the approved and actual baseline. The surveillance framework shall address the following:
    - methods of determining what audits are to be performed
    - frequency of audits
    - how identified inconsistencies and noncompliances are addressed and managed

- defined or identified processes that support the ASA requirements for the supply of assured, accurate and timely configuration information in the required formats to configuration information custodians
- have arrangements to provide the ASA with the following information:
  - access to configuration management records
  - access to product configuration information held
  - configuration and configuration change reports as required

9.3. AEO system requirements

AEOs engaged to perform configuration changes or maintenance to TfNSW transport assets shall have a documented configuration management system appropriate to the services they are providing and the conditions of their engagement.

Systems shall be consistent with AS ISO 10007. The system shall be compatible with this configuration management plan and any applicable configuration management plans of the party that has engaged the AEO.

Where an AEO has been engaged as the party responsible for network configuration and asset assurance of proposed or current TfNSW transport assets, the requirements for that role apply.

10. Configuration baselines

Configuration baselines serve as the basis for defining change, for conducting verifications and for other management purposes. For managing configuration changes in TfNSW, three standard baselines are identified:

- requirements baseline
- approved-for-construction baseline
- product baseline

During the process of implementing a configuration change, other interim configuration baselines may be established for management purposes as determined appropriate by party responsible for managing the change.

10.1. Requirements baseline

The requirements baseline is established when an asset change is defined to meet a business need. The change is generally considered as defined when a system requirements specification is approved by all relevant stakeholders. An 'asset change' can be a change to an existing asset or creation of a new asset. Business stakeholders and other stakeholders affected by the change shall have agreed to a set of requirements as adequately satisfying their needs.

The requirements baseline is associated with gate 1.

10.2. Approved-for-construction baseline

The approved-for-construction baseline is established when a design has received all necessary configuration management and technical approvals to be issued for construction. Technical approvals include concessions and evidence that the ASA has no objection to nonconformances to ASA requirements.

The approved-for-construction baseline is associated with gate 3.

10.3. Product baseline

The product baseline is established when a physical and functional audit of the constructed asset has been completed, any nonconformances rectified or accepted by the TfNSW CMAAC following the provision of evidence that the ASA has no objection to the nonconformance and all as-built configuration documents lodged in appropriate ASA nominated information systems. This usually occurs at the acceptance of a new or an altered asset for normal service.

The product baseline defines the design that is introduced and used in the operational phase. The product baseline is the basis for control of any future change to the asset.

Baselines established for current assets are equivalent to the product baseline.

The product baseline may also be referred to as the 'as-built' baseline.

The product baseline is associated with gate 5.

11. Type approved products and standard designs

Type approved products and standard designs may be used as inputs in to a configuration change. Such items have been through a process of assessments to provide assurance that they are suitable for use on the TfNSW network. Classification as a type approved product or a standard design may be used as a supporting argument for assuring a configuration change however assessments need to still be conducted to assure that the type approved product or standard design is appropriate for the given application.

12. Configuration management gates

Seven defined configuration gates have been established for the management of configuration changes. The gates are identified numerically from gates 0 to gate 6. All stages of an asset life cycle are covered by the defined gates. Responsibility for gates may vary during the life of an asset. The configuration management gates are shown relative to the asset life cycle in Figure 2. A representation of configuration management gates relative to asset life cycle activities is included in Appendix A.

Assurance to the CMAAC or its delegate shall be provided by the accountable party at the nominated gates throughout the course of an asset's life in order for the project to progress past through each gate. The progressive and continuous assurance of configuration changes throughout the life cycle of the asset provides continuous assurance to TfNSW that new, altered, and existing assets are in a known state and condition and delivering expected outcomes.

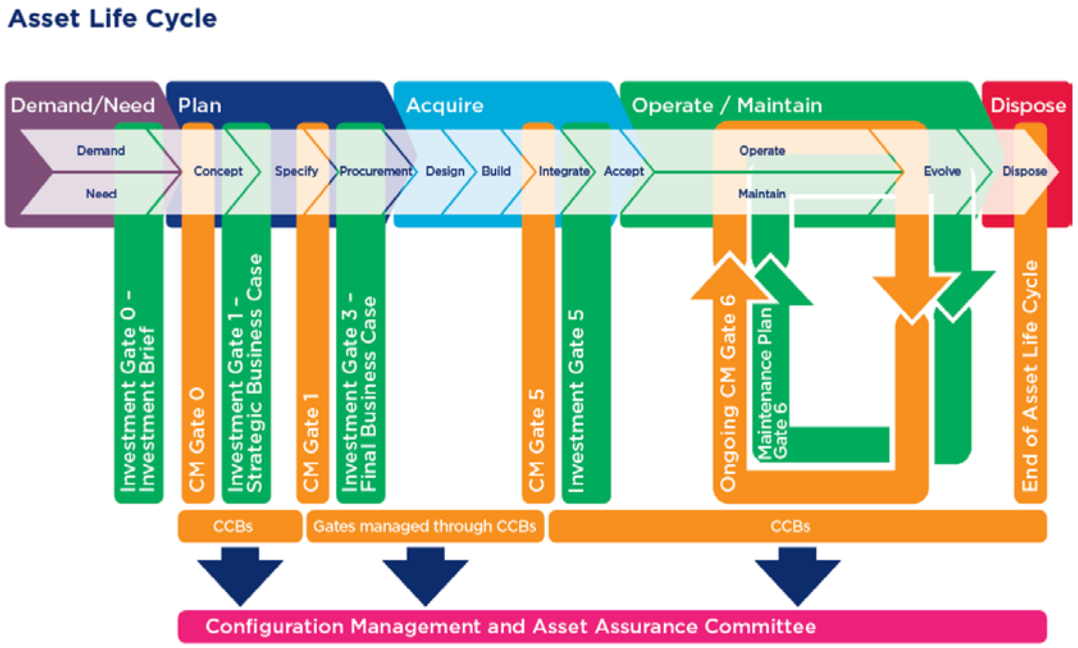


Figure 2 - Assurance gates throughout asset life cycle

12.1. Gate 0 – Initiation

This initial gate occurs after the purpose of a configuration change defined and initial business requirements developed.

The party accountable for the development of the planning of the configuration change shall be accountable for progressing through this gate. Within TfNSW, this is usually Planning and Programs Division.

12.1.1. Minimum requirements for gate 0

Responsible organisations shall provide the CMAAC with evidence that the following has been performed:

- initial high level business requirements including an analysis of need and demand
- high level expectations of the solution from the perspective of the user is understood, such as in the form of a concept of operations document
- initial assurance and governance plan that demonstrates a systems approach to defining a solution and producing the assurance evidence required for Gate 1. The plan shall include demonstration that the following aspects will be addressed:

  - governance and assurance arrangements for how the development of the solution will be progressively assured over the plan phase of the asset life cycle, including at the point when a preferred solution is identified
  - alignment with network strategy
  - whole of life costs
  - effects on reliability, availability, maintainability and safety of the network
  - a risk based approach to decision making
  - development of solutions that are justifiable as safe SFAIRP
- consideration of the risk of not proceeding with the proposed change

12.2. Gate 1 – Requirements complete

The 'requirements complete' gate occurs after the requirements of the preferred option have been well defined and are ready to be turned into a design.

The party accountable for the development of the planning of the configuration change shall be accountable for progressing through this gate. Within TfNSW, this is usually Planning and Programs Division.

12.2.1. Minimum requirements for gate 1

Responsible organisations shall provide the CMAAC with evidence that the following is in place, or has been performed:

- assurance and governance plan covering the configuration change project through to completion
- approved business requirements specification
- approved system requirements specification
- report to show stakeholders have been identified, consulted and have had their feedback addressed
- risk based decision making in optioneering
- the specified system is one which ensures that is safe SFAIRP
- reliability, availability, maintainability and safety (RAMS) assessments have been conducted
- whole of life costing assessments have been conducted

Requirements for assurance and governance plans are described in TS 10753: 2014 *Assurance and Governance Plan Requirements*.

12.3. Gate 2 – Initial design complete

This 'initial design complete' gate occurs at the point that a preliminary design has been completed.

The party accountable for the delivery of the design of the configuration change shall be accountable for progressing through this gate. This is usually the organisation, business unit, or agency responsible for the acquisition stage of the configuration change.

12.3.1. Minimum requirements for gate 2

Responsible organisations shall provide the CMAAC with evidence that the following is in place, or has been performed:

- approved concept design
- project hazard log
- assessment of safety risk for the given scope to demonstration that it is safe SFAIRP
- independent safety assessment report for significant configuration changes
- stakeholders have been identified, consulted and have had their feedback addressed
- reliability, availability, maintainability, and safety (RAMS) assessments have been conducted to a level appropriate to the significance of the proposed change
- whole of life costing assessments have been conducted to a level appropriate to the significance of the proposed change
- all appropriate technical approvals have been identified and obtained

12.4. Gate 3 – For construction

The 'for construction' gate occurs at the point when the detailed design has been developed and the project is ready to progress to construction.

The party accountable for the delivery of the design of the configuration change shall be accountable for progressing through this gate. This is usually the organisation, business unit, or agency responsible for the acquisition stage of the configuration change.

12.4.1. Minimum requirements for gate 3

Responsible organisations shall provide the CMAAC with evidence that the following is in place, or has been performed:

- detailed designs that have been approved for construction
- project hazard log

- safety interface arrangements where relevant
- assessment of safety risk for the given scope, generally a safety assurance report (SAR) or safety in design report
- independent safety assessment report for significant configuration changes
- safety assurance argument including SFAIRP demonstration
- stakeholders have been identified, consulted and have had their feedback addressed
- demonstration that approved business requirements specifications and systems requirements specifications have been met
- reliability, availability, maintainability and safety assessments have been conducted to a level appropriate to the significance of the proposed change
- whole of life costing assessments have been conducted to a level appropriate to the significance of the proposed change
- technical approvals have been identified and obtained
- identification of configuration information that is to be delivered to the owners, operators and maintainers
- assurance of completeness and delivery of approved-for-construction (AFC) drawings to the relevant custodian in a format meeting drawing requirements

12.5. Gate 4 – Ready for testing

The 'ready for testing' gate occurs at the point when a transport asset has been altered or added and is ready to progress to testing. Where there are multiple stages in the testing phase, of which some may be particularly high risk, separate submissions may be appropriate.

The party accountable for the delivery of the new or altered asset shall be accountable for progressing through this gate. Within TfNSW, this is usually the business unit or agency responsible for the acquisition stage of the configuration change.

12.5.1. Minimum requirements for gate 4

Responsible organisations shall provide the CMAAC with evidence that the following is in place, or has been performed:

- project hazard log
- assessment of safety risk for the given scope
- independent safety assessment report for significant configuration changes
- safety assurance argument including SFAIRP demonstration as required by TS 20001: 2013

- stakeholders have been identified, consulted, and have had their feedback addressed
- demonstration that approved business requirements specifications and systems requirements specifications have been met
- technical approvals have been identified and obtained; deviations from ASA requirements shall be supported by evidence of an ASA issued concession or no objection to nonconformances; and evidence of adequate risk controls for the deviations
- inspection and test plans and strategy to a level appropriate to the significance of the proposed change

12.6. Gate 5 – Asset acceptance

The asset acceptance gate occurs at the point shortly before the handover of the asset from the project team with responsibility for delivering the asset to the maintainer. This applies even if both parties are from the same organisation.

The party accountable for the delivery of the new or altered asset shall be accountable for progressing through this gate. Within TfNSW, this is usually the business unit or agency responsible for the acquisition stage of the configuration change.

Asset acceptance shall be based on documented evidence provided to TfNSW that assure it that the proposed or current assets are appropriately fit for purpose, reliable, available, maintainable, safe, and assessed for whole of life costs.

12.6.1. Minimum requirements for gate 5

Responsible organisations shall provide the CMAAC with evidence that the following is in place, or has been performed:

- project hazard log
- operational readiness arrangements or equivalent as appropriate to the nature of the project
- assessment of safety risk for the given scope, generally a safety assurance report (SAR)
- identification of residual safety risks
- stakeholders have been identified, consulted and have had their feedback addressed
- demonstration that approved business requirements specifications and system requirements specifications have been met
- reliability, availability, maintainability and safety (RAMS) assessments have been conducted to a level appropriate to the significance of the proposed change

- whole of life costing assessments have been conducted to a level appropriate to the significance of the proposed change
- technical approvals have been identified and obtained; deviations from ASA requirements shall be supported by evidence of an ASA issued concession or no objection to nonconformances, and evidence of adequate risk controls for the deviations
- operational matters have been addressed
- identification of configuration information that that has been delivered to configuration information custodians and schedule for delivery of outstanding configuration information
- configuration information delivered has been assured as being technically correct and in the correct format

12.7. Gate 6 – Asset assurance review

The asset assurance review gate occurs annually, unless otherwise agreed or determined by the ASA. This gate is a demonstration by a maintainer that TfNSW transport assets under the control of the maintainer has been appropriately managed and provides the CMAAC with assurance that planned configuration changes are being properly managed. The evidence of assurance shall cover the management of the configuration, safety risks and consideration of whole of life reliability, maintainability, availability and whole of life costs.

The party accountable for maintaining the assets is accountable for progressing through this gate.

12.7.1. Minimum requirements for gate 6

Responsible organisations shall provide the CMAAC with evidence that the following is in place, or has been performed:

- demonstration that a risk based approach has been applied in developing the asset maintenance plan and annual works plan
- assurance argument that the asset maintenance plan and annual works plan provided best maintains the integrity of the transport network balanced against TfNSW objectives and the maintenance requirements
- demonstration that the previous asset maintenance plan and annual works plan has been achieved and that resulting network configuration ensures safety SFAIRP through assurance and integrity reporting
- demonstration of appropriate assessment of impact for all changes made to the network through maintenance or otherwise

- demonstration of an appropriate level of surveillance of the assets under its control, this may include functional and physical audits
- progressive assurance throughout the year on maintenance carried out and performance
- demonstrate that applicable configuration management plans have been complied with and are effective

13. Categorisation of configuration change significance

All configuration changes to TfNSW transport assets shall demonstrate adequate assurance that the configuration change has been properly managed. As a considerable number of configuration changes occur on the TfNSW transport network, the authority to make decisions that affect network configuration changes is managed through delegations.

Arrangements for delegations are required to provide the CMAAC with confidence that appropriate levels of governance are applied to each configuration change.

To facilitate a consistent approach for determining the level of assurance required by the CMAAC, a three level classification is used to determine the significance of the configuration change. The categorisation will determine the minimum procedural requirements for obtaining acceptance of a configuration change request.

Configuration changes are classified as significant, moderate, or minor.

13.1. Assessment of configuration change classification

The classification of the configuration change shall be determined by the scope of the change being assessed and not the overall project it is part of though the impact of the change on the overall transport network shall form part of the consideration. For example, the integration of an additional simple and common asset to the transport network may occur as part of an overall project but that asset may potentially introduce significant risks or impacts to the network as a whole. That configuration change shall thus be assessed within the broader network context. This may be particularly relevant where the new asset introduces new interfaces between other assets on the network.

The assessment of a configuration change shall be made as early as possible in advance of a submission to gate 1 and gate 5. The need to assess the significance of a configuration change at other stages is dependent on any identified arrangements within the assurance and governance plan of a project, or arrangements within an applicable configuration management plan accepted by the ASA CCB.

13.2. Significant configuration change classification

Unless otherwise indicated by the CMAAC a configuration change is considered significant if any of the following criteria are met:

- safety significant when assessed against the criteria defined in the TS 20001: 2013 and 20-FT-388 *Initial Safety Change Assessment*. The criteria listed in 20-FT-388 *Initial Safety Change Assessment* are used to assess the individual configuration change, not the overall project.
- high public profile, significant direct impact on public using a part of a transport mode or significant impact on a large community
- medium risk or higher as assessed under the 30-ST-164 *TfNSW Enterprise Risk Management Standard*
- introduces a potentially significant long term, operational, or maintenance impact. Considerations may include cost, unique resources, logistics and scheduling.

Examples of configuration changes that will generally be considered significant include those listed below:

- new major transport interchange
- new transport fleet (such as ferries, buses, rolling stock)
- new ferry wharves or train stations
- major changes to the configuration of high patronage ferry wharves or train stations
- new rail line
- major rail re-signalling or changes to control systems

13.3. Moderate configuration change classification

Unless otherwise indicated by the CMAAC a configuration change is considered moderate if all of the following criteria are met:

- not safety significant when assessed against the criteria defined in the TS 20001: 2013, 20-FT-388 *Initial Safety Change Assessment*. The criteria listed in 20-FT-388 *Initial Safety Change Assessment* are used to assess the individual configuration change, not the overall project.
- does not have a high public profile, significant direct impact on public using a part of a transport mode or significant impact on a large community
- low risk as assessed under the 30-ST-164 *TfNSW Enterprise Risk Management Standard*

- is unlikely to introduce a potentially significant long-term change in operational or maintenance requirements. Considerations may include cost, unique resources, logistics, and scheduling.
- does not meet the classification criteria of a minor configuration change

Examples of configuration changes that will generally be considered moderate include those listed below:

- electrical substations
- car parks
- railway turnouts
- bridge renewals

13.4. Minor configuration change classification

Unless otherwise indicated by the CMAAC a configuration change is considered minor if all of the following criteria are met:

- not safety significant when assessed against the criteria defined in the TS 20001: 2013, 20-FT-388 *Initial Safety Change Assessment*. The criteria listed in 20-FT-388 *Initial Safety Change Assessment* are used to assess the individual configuration change, not the overall project.
- minor or no direct impact to public
- minimal impact to the functionality, reliability or availability of the network
- low risk as assessed under the 30-ST-164 *TfNSW Enterprise Risk Management Standard*
- is a routine or common configuration change
- does not require the application of operational or maintenance concepts that are new to the operator or maintainer
- does not have significant adverse effect on the maintenance activities of the maintainer or the spares that the maintainer is to hold

Examples of configuration changes that will generally be considered minor include those listed below:

- bus shelters
- ramps, escalators, and lifts
- lighting
- fencing

- cable relocation
- drainage

13.5. Configuration change significance and CMAAC engagement

Significant configuration change requests at gate 1 and gate 5 shall be presented to the CMAAC unless otherwise determined on a case by case basis by the CMAAC.

Decisions for all other configuration change requests may be delegated to a CCB or other approved party in accordance with configuration management plans approved by the ASA CCB. Where no ASA CCB approved arrangements for delegation have been made and where the CMAAC has not given a specific directive, then the configuration change request is to be presented to the CMAAC for acceptance.

Where a moderate configuration change is accepted by a delegated party at gate five, the configuration change manager shall prepare a notification of delegated asset acceptance to the CMAAC unless other arrangements have been approved by the ASA CCB. The notification shall be prepared on a standard template provided by the ASA and include a brief summary of the assets accepted and the evidence available as described under the minimum requirements for progressing past gate five described in this document.

For all other delegated configuration changes, reports shall be provided to the ASA, for provision to the CMAAC, as assurance that due process has been followed. Reports will usually be provided by the delegated CCB that has made the decision about the configuration change.

At any time, the CMAAC or the ASA may request a configuration change manager or maintainer to present a configuration change request to the CMAAC or to provide evidence that demonstrates proper management of any part of a configuration change.

The example shown in Figure 3 represents a typical arrangement for projects with multiple work packages, handover events, and configuration management gates.

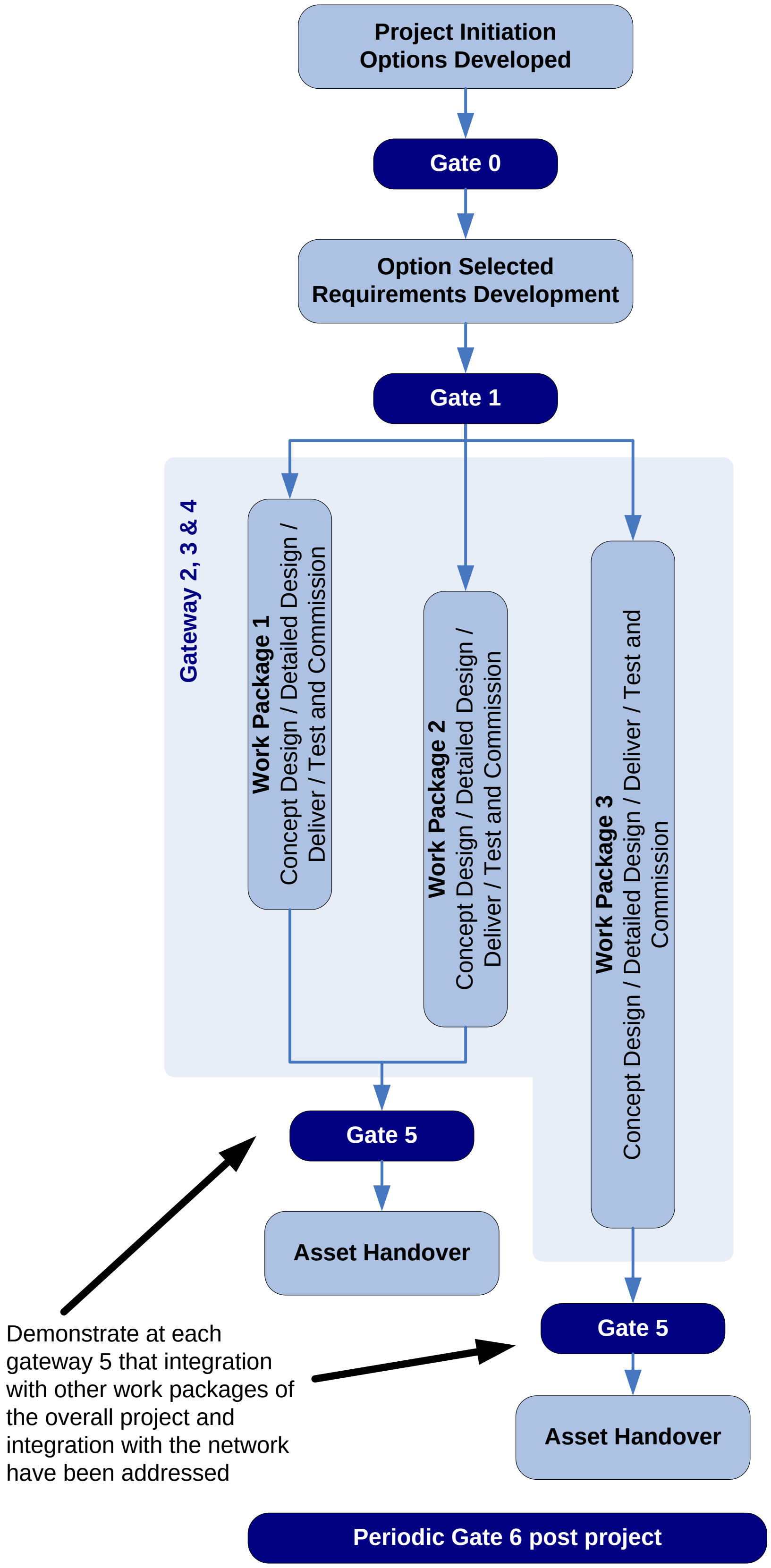

Project Initiation
Options Developed
Gate 0
Option Selected
Requirements Development
Gate 1
Gateway 2, 3 & 4
Work Package 1
Concept Design / Detailed Design / Deliver / Test and Commission
Work Package 2
Concept Design / Detailed Design / Deliver / Test and Commission
Work Package 3
Concept Design / Detailed Design / Deliver / Test and Commission
Gate 5
Asset Handover
Gate 5
Asset Handover
Demonstrate at each gateway 5 that integration with other work packages of the overall project and integration with the network have been addressed
Periodic Gate 6 post project

Figure 3 - Example of gates relative to project activities

14. Configuration identification

Configuration identification shall occur progressively throughout the design process as functional and physical characteristics are documented in successively greater levels of detail.

The primary objective of configuration identification is to define accurately the approved configuration and to provide a basis for change control. The design status of an asset may be defined at any time by reference to a configuration baseline.

Configuration identification consists of the following aspects:

- determining asset structure and selecting items to which configuration management activities will be applied
- documenting configuration items
- assigning unique codes to configuration items and their documents
- establishing configuration baselines

Configuration items are selected by breaking down the system to a level of detail that is adequate by considering the following aspects:

- the maintenance activities to be performed
- a configuration item's criticality
- interfaces to other elements
- procurement conditions

Configuration information shall set out all functional and physical characteristics of the configuration items and their interfaces to a level of detail relevant to the functionality, reliability, and maintainability of the TfNSW transport assets.

All software that forms part of the configuration or is included in configuration documents shall be identified by a formal version and release number.

15. Change control

Change control is the process of managing a configuration change. TfNSW applies change control to assure itself that changes to its transport network are properly managed.

15.1. Change control procedures

All change control shall comply with the basic procedures shown in Figure 4.

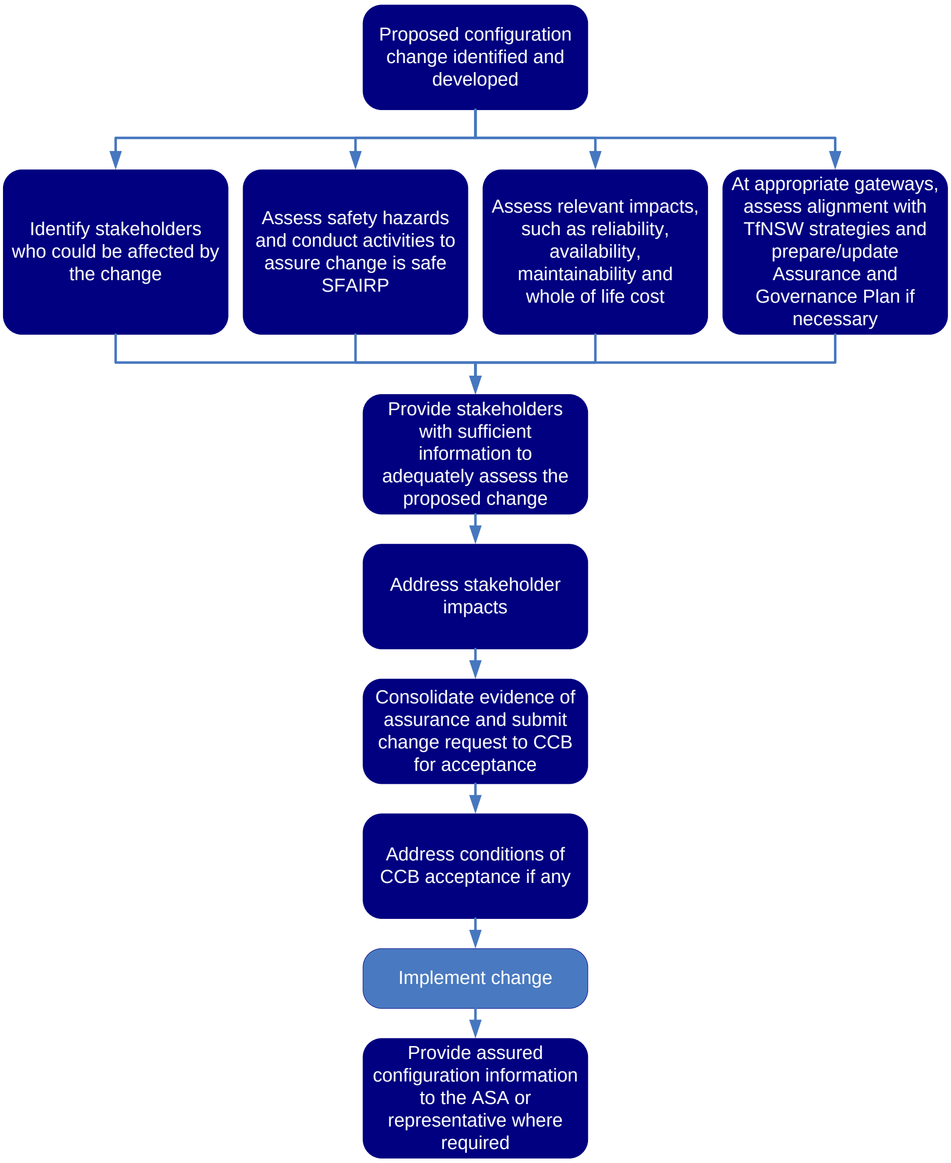

Proposed configuration change identified and developed
Identify stakeholders who could be affected by the change
Assess safety hazards and conduct activities to assure change is safe SFAIRP
Assess relevant impacts, such as reliability, availability, maintainability and whole of life cost
At appropriate gateways, assess alignment with TfNSW strategies and prepare/update Assurance and Governance Plan if necessary
Provide stakeholders with sufficient information to adequately assess the proposed change
Address stakeholder impacts
Consolidate evidence of assurance and submit change request to CCB for acceptance
Address conditions of CCB acceptance if any
Implement change
Provide assured configuration information to the ASA or representative where required

Figure 4 - Basic change control procedure applicable at each gate

The basic change control procedures is intended to apply at each submission gate but should be adapted and documented to suit specific situations.

All change control procedures shall achieve the following objectives:

- earliest control of changes
- effective consultation with stakeholders
- change control decisions at the appropriate management level
- assurance that an audit trail of stakeholder consultation, impact resolution and configuration control decisions is maintained
- configuration information that is appropriately and efficiently updated in the required format and updated in the appropriate system

15.2. Stakeholder identification

For any configuration change request, a process of stakeholder identification and management is required. Stakeholders or their nominated representatives shall be included on the stakeholder list for a configuration change request whenever there is a possibility that their area of responsibility may be potentially affected, positively or adversely.

In considering stakeholders to a proposed change, the following effects shall be considered:

- strategic direction of TfNSW
- safety
- operation and maintenance of the asset throughout the whole asset life
- interfacing TfNSW transport operations or assets
- third party operations, assets or other areas of responsibility, (such as local governments, utilities, transport providers)
- environment and heritage
- customers, individuals or businesses
- commuters and community

15.3. Configuration change requests

All additions to, and deletions from, the existing asset configuration and renewals that are not exactly identical replacements, including repositioning of existing assets, are configuration changes.

Configuration change requests shall be submitted to a CCB, or delegate where available, for determination in the following circumstances:

- introduction or removal of a configuration item
- changes to the performance or life cycle maintenance profile of a configuration item
- maintenance that involves changes to the existing configuration

Each proposed network configuration change that progresses towards the requirement for configuration change request approval, shall be registered as a configuration change request and be assigned a unique number for traceability. A configuration change is not considered complete until the configuration change has been implemented including all conditions applied as part of the configuration change request approval and all current product configuration information relevant to the configuration change provided to configuration information custodians in the correct format.

15.4. Implementation of configuration control board decisions

Effective implementation of change control requires CCB decisions be appropriately implemented.

CCB decisions shall meet the following criteria:

- fully and accurately recorded and documented
- communicated by the CCB or representative as soon as practicable to the configuration change manager and then by the configuration change manager to other parties responsible for implementation
- implemented strictly in accordance with the CCB decision, including any conditions of approval

The configuration change manager is to ensure that a complete audit trail of the implementation process is kept by all parties with responsibility for the implementation, and that the record is made available to auditors, investigators and other authorised persons.

15.5. Out-of-session and delegated configuration change request approvals

Where arrangements for the approval of configuration change requests outside of a regular CCB meeting are to be made available, such arrangement shall be documented and be approved in an approved configuration management plan.

15.6. Change control registration system

A system for recording configuration change requests shall be applied by parties managing such requests.

All configuration change requests shall be assigned a number registered in a change control recording system and that number shall be unique across all parties involved in network configuration management of TfNSW transport assets.

The ASA is the owner of the number and numbering system but may delegate assignment and management of numbers.

15.7. Submissions to the CMAAC

The ASA is to be notified of any upcoming configuration change requests that are to be presented to the CMAAC as early as possible. The notification allows provides the CMAAC and the ASA with visibility and supports traceability of upcoming agenda items.

Configuration change request submissions to the CMAAC shall be provided to the ASA, as secretary to the CMAAC prior to presentation to the CMAAC. Configuration change managers shall meet the following schedule requirements when intending to present to the CMAAC:

- early draft of configuration change submissions to be provided to the ASA at least six weeks prior to expected CMAAC presentation
- final configuration change submission to be provided to the ASA at least two weeks prior to expected CMAAC presentation

15.8. Record keeping and audit trail

Sufficient records shall be retained to demonstrate clearly that due process has been followed in obtaining signoff from stakeholders, CCB approvals, implementing decisions and any other configuration management activity.

16. Configuration status accounting

Configuration status accounting is the recording and reporting of the product configuration information, the status of proposed or in progress changes to provide a traceable record of activities. It is applied in conjunction with configuration identification and change control.

Configuration status accounting includes the following tasks:

- storage and control of product configuration information, including the receipt and issue of configuration documents
- maintaining records of configuration documents and identification codes
- maintaining records of the implementation status of proposed and approved configuration changes

Configuration change managers are responsible for providing updated configuration information for configuration items affected by the configuration change.

Configuration data shall be provided without delay to the configuration information system custodian after the information is available. All required configuration information that accurately reflects the as-built configuration baseline shall be provided prior to the completion of a project. The information provided shall be in accordance to published ASA requirements and requirements provided by configuration information custodians as the party managing the information on behalf of TfNSW.

Parties responsible for the delivery of configuration information to configuration information custodians shall assure that the information is correct and presented in the required format. Arrangements to provide this assurance shall be documented.

Configuration information custodians are responsible for confirming that product configuration information provided by configuration change managers is entered in to the appropriate configuration information system.

Configuration identification recovery shall be used if inconsistencies or deficiencies are identified during configuration status accounting.

16.1. Product configuration information owned by ASA

A range of product configuration information is in existence and is continually developed by TfNSW and parties performing work for TfNSW. The ASA is the delegated owner of product configuration information for TfNSW transport assets. Configuration information within this scope is the information describing the transport assets that is required for effectively understanding, maintaining, and modifying the physical and functional characteristics of transport assets.

Information that is created or collected to meet local or temporary requirements that is additional to that required for delivery to configuration information custodians is not generally considered product configuration information owned by the ASA. Where it is unclear if the ASA is the owner of the product configuration information, the ASA will make a determination.

The ASA will develop a register of known systems that hold product configuration information that it owns.

16.2. Configuration information systems and custodians

The ASA does not generally own configuration information systems. Configuration information system custodian services will generally be provided to the ASA by nominated AEOs. Such services include providing appropriate repositories to hold and manage ASA-owned product configuration information. The ASA will develop a register of known systems that hold product configuration information and the system custodians that manage that information.

The custodian of a configuration information system is the party responsible for managing a configuration information repository regardless of ownership. Configuration information system custodians shall meet the requirements of this and any other relevant TfNSW document, including any agreed performance requirements.

Requirements for the provision and management of the ASA-owned configuration information shall be owned by the ASA but may be delegated or managed collaboratively with the configuration information custodian as appropriate.

17. Configuration identification recovery

Configuration identification recovery is the correction of inconsistencies between the physical asset and its product configuration information when an inconsistency is detected.

Depending on the nature of the inconsistency, either the product configuration information or the physical asset will need to be changed.

Configuration identification inconsistencies fall into four broad categories:

- product configuration information does not match the physical item
- conflicting sets of configuration information exist for the same configuration item
- configuration documents do not exist for an item
- inconsistencies exist between configuration documents

The need for configuration identification recovery may be determined from configuration identification, change control, configuration status accounting, or surveillance activity.

Parties responsible for the network configuration of TfNSW transport assets are to be pro-active about configuration identification recovery for assets they have responsibility for, and have in place procedures to restore the integrity of the system when discrepancies are detected.

If the inconsistency is caused by a project in progress, responsibility for conducting the configuration identification recovery lies with the party in control of the project.

Configuration identification recovery requires identifying the approved baseline relating to the inconsistency and rectifying the inconsistency to the approved baseline by conducting one or more of the following activities:

- altering the configuration item
- altering the configuration data
- obtaining business, technical, and configuration management approval for a new baseline

18. Configuration surveillance

Surveillance of configuration management includes any activity that forms part of an assessment of the status of the application of configuration management. Where surveillance activities identify potential failures in the process or errors in information, activities are to be implemented by the responsible entity to manage the identified issue.

As part of configuration management surveillance, the ASA, AEOs, and configuration information custodians shall plan and perform audit activities appropriate to their role. Audits shall be conducted on the application of configuration management including the process, quality of configuration information, and its relationship to actual and approved baselines as appropriate.

18.1. Configuration audits

Configuration audits are used to determine whether configuration items conform to approved product configuration information. A functional configuration audit is conducted to determine whether a configuration item has the performance and functional characteristics specified in its functional baseline. A physical configuration audit is conducted to determine whether the as-built product conforms to its constructed baseline. Process audits are conducted to assess compliance with approved processes.

The ASA, parties responsible for the configuration of TfNSW transport assets, and configuration information custodians shall establish and implement configuration audit plans as part of surveillance activities.

Auditors are responsible for the following tasks:

- developing an audit plan showing resources, activities scheduled and responsibilities
- identifying in the audit plan which configuration items are to be audited and what criteria are to apply
- performing the audit including any reviews, tests and inspections
- specifying the actions arising from the audit
- keeping records and preparing the audit report

Audit plans shall address the validation of assets handed over at the completion of a change against the configuration documents, including approved design where applicable.

19. Supporting documents and tools

Additional documents, forms, and tools that support the configuration management processes are published by the ASA or its representatives. Unless otherwise prescribed by other documents or CCB advice, such supporting material shall be used for configuration management as appropriate and intended.

Appendix A Standard configuration control gates

The configuration management gates relative to the life cycle stages and project activities are shown in this diagram of the asset life cycle (Figure 5).

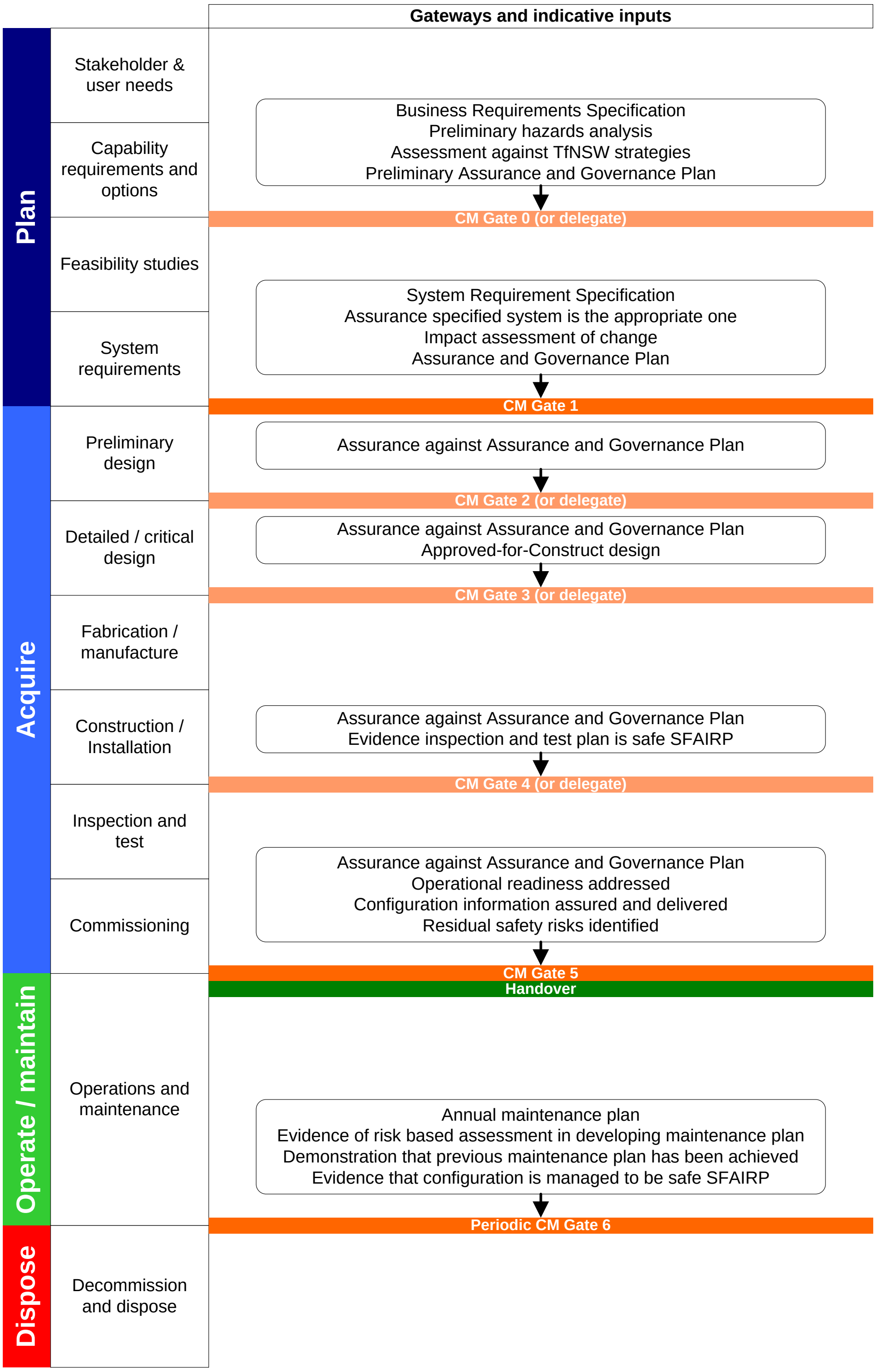

Gateways and indicative inputs
Plan
Acquire
Operate / maintain
Dispose
Stakeholder & user needs
Capability requirements and options
Feasibility studies
System requirements
Preliminary design
Detailed / critical design
Fabrication / manufacture
Construction / Installation
Inspection and test
Commissioning
Operations and maintenance
Decommission and dispose
Business Requirements Specification
Preliminary hazards analysis
Assessment against TfNSW strategies
Preliminary Assurance and Governance Plan
CM Gate 0 (or delegate)
System Requirement Specification
Assurance specified system is the appropriate one
Impact assessment of change
Assurance and Governance Plan
CM Gate 1
Assurance against Assurance and Governance Plan
CM Gate 2 (or delegate)
Assurance against Assurance and Governance Plan
Approved-for-Construct design
CM Gate 3 (or delegate)
Assurance against Assurance and Governance Plan
Evidence inspection and test plan is safe SFAIRP
CM Gate 4 (or delegate)
Assurance against Assurance and Governance Plan
Operational readiness addressed
Configuration information assured and delivered
Residual safety risks identified
CM Gate 5
Handover
Annual maintenance plan
Evidence of risk based assessment in developing maintenance plan
Demonstration that previous maintenance plan has been achieved
Evidence that configuration is managed to be safe SFAIRP
Periodic CM Gate 6

Figure 5 - Standard configuration control gates for full asset life cycle