TS 00087.1:1.0

Procedure

Asset Criticality Assessment for Technology Systems

Part 1: Procedure

Issue date: 04 September 2023

Effective date: 04 September 2023

Disclaimer

This document has been prepared by Transport for NSW (TfNSW) specifically for its own use and is also available for use by NSW public transport agencies for transport assets.

Any third parties considering use of this document should obtain their own independent professional advice about the appropriateness of using this document and the accuracy of its contents. TfNSW disclaims all responsibility and liability arising whether directly or indirectly out of or in connection with the contents or use of this document.

TfNSW makes no warranty or representation in relation to the accuracy, currency or adequacy of this document or that the document is fit for purpose.

The inclusion of any third party material in this document, does not represent an endorsement by TfNSW of any third party product or service.

For queries regarding this document, please email Transport for NSW Asset Management Branch at standards@transport.nsw.gov.au or visit www.transport.nsw.gov.au

Document information

Owner:	Director Telecom Engineering Asset Management Safety, Environment and Regulation
Mode:	Multimodal
Discipline:	Security – Information and Cyber

Document history

Revision	Effective date	Summary of changes
1.0	04/09/2023	First issue.

Preface

Under the *NSW Cyber Security Policy* (CSP), NSW Government departments and public service agencies are required to provide a list of their 'crown jewels'. Historically, different approaches have been used across Transport to determine which assets are 'crown jewels'.

Transport completes business impact assessments as part of business continuity to identify critical services and processes across the entire cluster, and identify resources and contingencies required to continue and resume these critical services and processes in a crisis.

Whilst these assessments identify resource dependencies including technology assets, there is no TfNSW procedure for determining the relative criticality of these assets to support targeted uplift investments, risk buy-down, and assurance activities.

This document describes the procedure to perform asset criticality assessments for technology systems to meet relevant information and cyber security regulatory, policy, and compliance obligations.

This process determines the level of criticality of the asset and provides mappings to related classifications within regulatory and policy instruments and other standards.

This document also describes the onboarding to and offboarding from TfNSW information and cyber security management systems.

The terms 'normative' and 'informative' are used in asset standards to define the application of the appendices to which they apply. A 'normative' appendix is an integral part of an asset standard, whereas an 'informative' appendix is only for information and guidance.

This document is a first issue.

Table of contents

1 Scope

This document describes the procedure to perform asset criticality assessments for technology systems to meet relevant information and cyber security regulatory, policy, and compliance obligations.

This process determines the level of criticality of the asset and provides mappings to related classifications within regulatory and policy instruments and other standards.

This document covers all technology systems irrespective of whether the system is classified as information technology (IT) or operational technology (OT). The scope includes all technology systems such as computers, computer systems, computer networks, and computer data.

> Note: Other standards may describe these systems as programmable electronic or computer-based systems.

This document does not address governance, assurance, compliance, and risk management obligations or activities that follow from the assessment of an asset's criticality.

2 Application

This document applies to new and altered assets in the Plan stage of the asset life cycle.

This document also applies with retrospective application to existing assets in the Operate/Maintain stage of the asset life cycle.

This document applies to asset custodians, asset stewards, delivery partners, and service providers who are accountable or responsible for technology systems.

3 Referenced 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.

Transport for NSW standards

CPSt20000 *TfNSW Enterprise Risk Management Standard*

> Note: This document is not publicly available. To obtain access email standards@transport.nsw.gov.au

TS 00087.2 *Asset Criticality Assessment for Technology Systems Part 2: Form*

TS 04982 (T MU MD 20002 ST) *Risk Criteria for Use by Organisations Providing Engineering Services*

Other referenced documents

State of New South Wales *NSW Cyber Security Policy*

State of New South Wales *NSW Government Information Classification, Labelling and Handling Guidelines*.

4 Terms, definitions and abbreviations

The following terms, definitions and abbreviations apply in this document.

ACSC Australian Cyber Security Centre

asset custodian the TfNSW Division accountable for the end to end lifecycle management and performance of assets (including asset condition, risk and reporting) on behalf of the asset owner to achieve agreed customer and community outcomes

asset steward the entity given the responsibility by an asset custodian to oversee part of the lifecycle process for an asset

business impact assessment activity to identify resources and contingencies required to continue or restore enterprise critical business functions and their business continuity priorities

CDPB Cyber Defence Portfolio Board

CISO Chief Information Security Officer, TfNSW

crown jewels the most valuable or operationally vital systems or information in an organisation. (Source: *NSW Cyber Security Policy*, State of New South Wales).

CSP *NSW Cyber Security Policy*

delivery partner an entity engaged to deliver products and services that may or may not be a TAO.

divisional or agency security representative security representative of division or agency nominated as a member of Transport cluster cyber management

IT information technology

OT operational technology; technology-based assets and services directly involved in the context of Transport's operations that can affect or influence safety, security, reliability, operational efficiency, service quality, and regulatory compliance

RASCI responsible, accountable, supported, consulted, informed

Responsible (R) – The role that does the work to complete the task or deliverable.

Accountable (A) – The role that is answerable for the correct and thorough completion of the task or deliverable. There is only one Accountability specified for each task or deliverable.

Supported (S) – The role that provides support to the task or deliverable and who assists the Responsible in the work.

Consulted (C) – The role(s) that are consulted on the task or deliverable and asked for their input, expert opinion.

Informed (I) – The role(s) that are kept informed on the status/completion of the task or deliverable.

service an individual or entity providing a service to TfNSW.

A Service Provider delivering self assured services under the TfNSW Technical Supplier Assurance Framework is referred to as a Delivery Partner and must hold technically assured organisation (TAO) accreditation.

TAO technically assured organisation

TCD Transport Cyber Defence, TfNSW

TfNSW Transport for NSW

5 Asset criticality assessment procedure

The procedure set out in this document shall be used to assess the asset criticality for the purpose of meeting relevant information and cyber security regulatory, policy, and compliance obligations.

An overview of the asset criticality assessment procedure is shown in Figure 1.

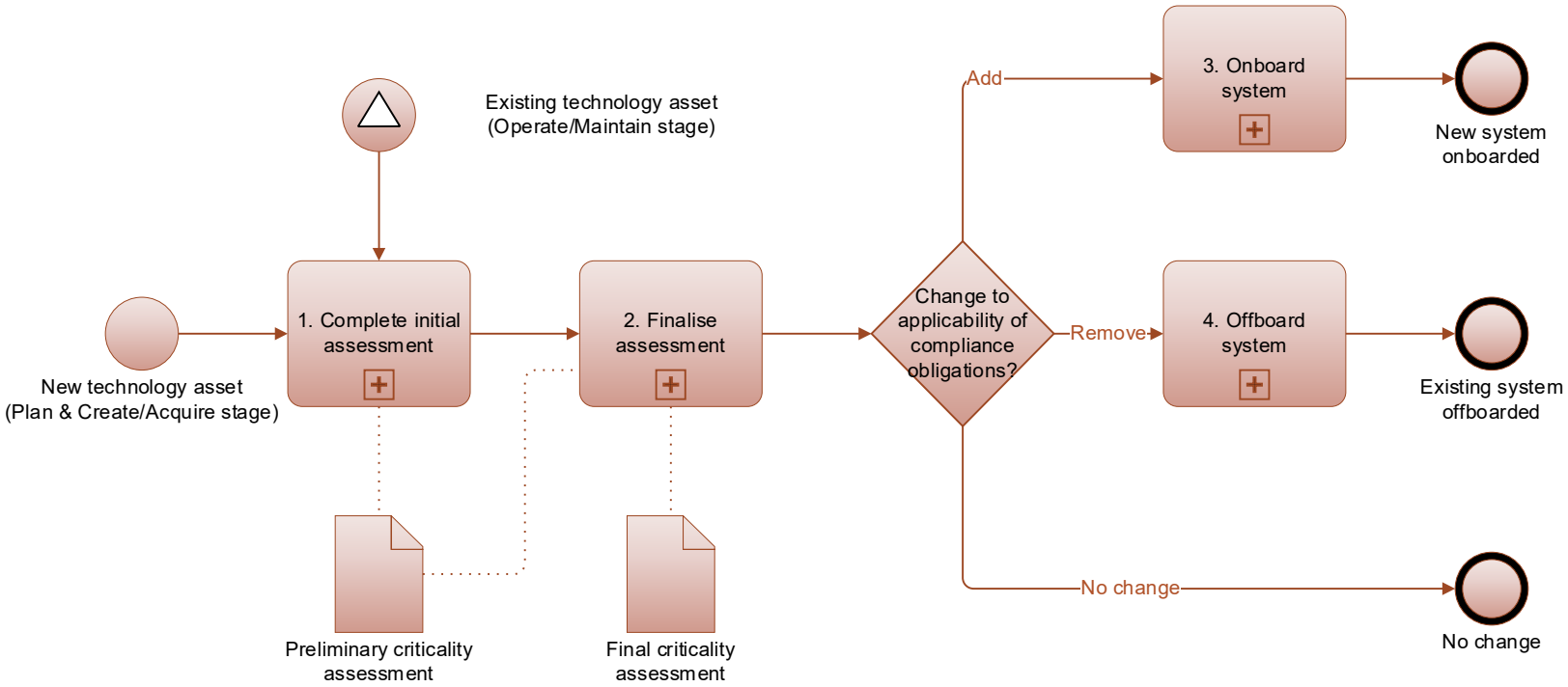


Figure 1 – Overview of asset criticality assessment procedure

The roles and responsibilities (with RASCI codes) for new and altered assets are summarised in Table 1.

Table 1 – Summary of roles and responsibilities – New and altered assets

Task	Asset Custodian	Asset Steward – Delivery	Asset Steward – Operate & Maintain	TCD Advisory	Divisional or Agency Security Representative	CISO	CDPB	TCD Compliance
Task 1: Complete initial assessment								
Task 1.1: Determine system scope	A	R	C	S	S			
Task 1.2: Identify business impact scenarios	A	R	C	S	S			
Task 1.3: Assess business impact scenarios	A	R	C	S	S			
Task 1.4: Determine criticality	A	R	C	S	S			
Task 2: Finalise assessment								
Task 2.1: Review cyber security impacts				A, R	S			
Task 2.2: Approve asset criticality assessment	A, R	S						
Task 2.3: Acknowledge asset criticality assessment						A, R	S	
Task 3: Onboard system						A		R
Task 4: Off board system						A		R

The roles and responsibilities (with RASCI codes) for existing assets are summarised in Table 2.

Table 2 – Summary of roles and responsibilities – Existing assets

Task	Asset Custodian	Asset Steward – Delivery	Asset Steward – Operate & Maintain	TCD Advisory	TfNSW Security & Risk Lead	CISO	CDPB	TCD Compliance
Task 1: Complete initial assessment								
Task 1.1: Determine system scope	A		R	S	S			
Task 1.2: Identify business impact scenarios	A		R	S	S			
Task 1.3: Assess business impact scenarios	A		R	S	S			
Task 1.4: Determine criticality	A		R	S	S			
Task 2: Finalise assessment								
Task 2.1: Review cyber security impacts				A, R	S			
Task 2.2: Approve asset criticality assessment	A, R		S					
Task 2.3: Acknowledge asset criticality assessment						A, R	S	
Task 3: Onboard system						A		R
Task 4: Off board system						A		R

5.1 Start events

Start events for this procedure include the following:

- new technology asset in the Plan and Create/Acquire stages of the asset life cycle.
- existing technology asset in the Operate/Maintain stage of the asset life cycle where one or more events have occurred that materially alters the basis of the previous assessment such as the following events:
    - new or changes to the following:
        - publication of a major revision of this document
        - business impact assessment identifies a technology system as a resource dependency, for example the system was not previously identified as a dependency of a critical service or process
        - regulatory or policy obligations, for example the system is subject to new or changed obligations which alters the risk assessment
        - enterprise risk management framework, for example the risk criteria or risk appetite changes which alters the risk assessment
    - observations, recommendations, and findings from the following which alter the business impact scenarios:
        - asset failure investigations
        - incident investigations
        - audits
        - cyber security exercises.

5.2 Data inputs

Data inputs to this task are described in following sections.

5.3 Task procedure

The steps for this task shall be performed as follows:

1. Perform complete initial assessment task, detailed in Section 6.
2. Perform finalise assessment task, detailed in Section 7.
3. If criticality assessment satisfies applicability criteria for information and cyber security compliance obligations but has not previously been onboarded to TfNSW information and

cyber security management systems then perform onboard system task, detailed in Section 8.

4. If criticality assessment does not satisfy applicability criteria for information and cyber security compliance obligations but has previously been onboarded to TfNSW information and cyber security management systems then perform offboard system task, detailed in Section 9.

5.4 Data outputs

Data outputs from this task shall include the following:

- Final criticality assessment
- System onboarded to or offboarded from TfNSW information and cyber security management systems.

6 Task 1: Complete initial assessment

An overview of the task is shown in Figure 2.

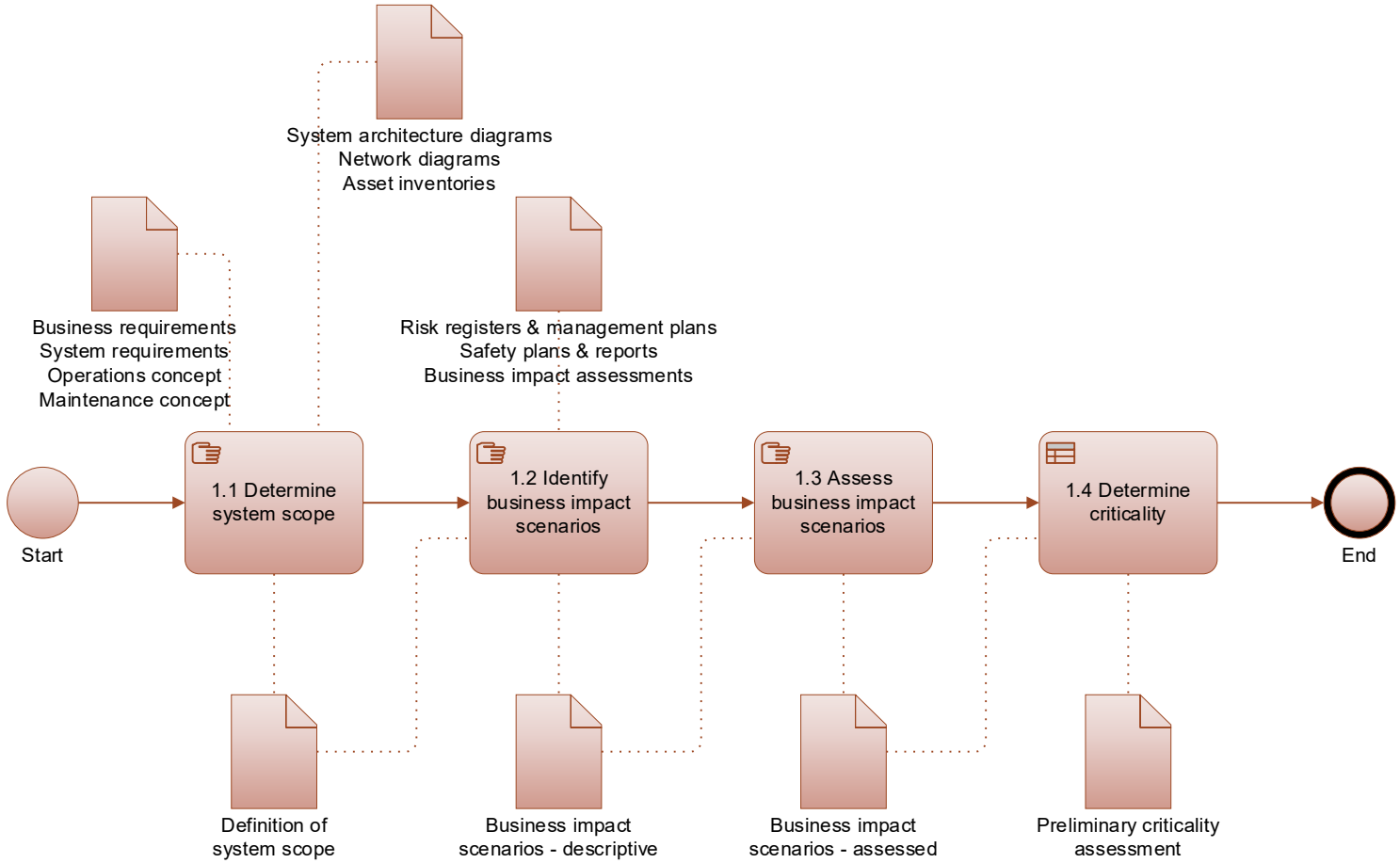


Figure 2 – Task 1: Determine initial assessment procedure

6.1 Task 1.1: Determine system scope

The purpose of this task is to define the scope of the system under consideration for assessment.

6.1.1 Data inputs

Data inputs to this task include the following:

- business requirements specifications
- system requirement specifications
- operations concept definition
- maintenance concept definition
- system architecture diagrams
- network diagrams
- asset inventories.

6.1.2 Task procedure

The steps for this task shall be performed as follows:

1. Identify the scope of the system under consideration (SuC) for assessment.
    - The scope of the system shall include all technology such as computers, computer systems, computer networks, and computer data.

    Note: Other associated assets such as buildings, facilities, rolling stock, vehicles, and vessels are not considered themselves to be technology systems, but may contain technology systems.

    - The scope of the system shall define the main parts of the system.
    - The scope of the system shall be consistent with asset and configuration item records.
2. Identify the physical security perimeter and access points to the system and main parts of the system.
3. Classify the information held within the system in accordance with the *NSW Government Information Classification, Labelling and Handling Guidelines*.
4. Classify the system as IT or OT.
5. Record the system scope using the TS 00087.2 form.

6.1.3 Data outputs

Data outputs from this task shall include the following:

- definition of system scope.

6.2 Task 1.2: Identify business impact scenarios

The purpose of this task is to identify business impact scenarios.

6.2.1 Data inputs

Data inputs to this task include the following:

- definition of system scope
- risk registers and management plans
- safety plans and reports
- enterprise business impact assessments.

6.2.2 Task procedure

The steps for this task shall be performed as follows:

1. Identify direct and immediate business impact scenarios as shown in Figure 3 for the risk events of loss of confidentiality, integrity, and availability for the system and main parts of the system.

   Note: Figure 3 shows the conceptual relationship and development of asset and business impacts over time using the Transport risk criteria. Some categories are not able to directly realise impacts within the operational window of one calendar day and develop over time. Other indirect impacts to the community or society may also arise.

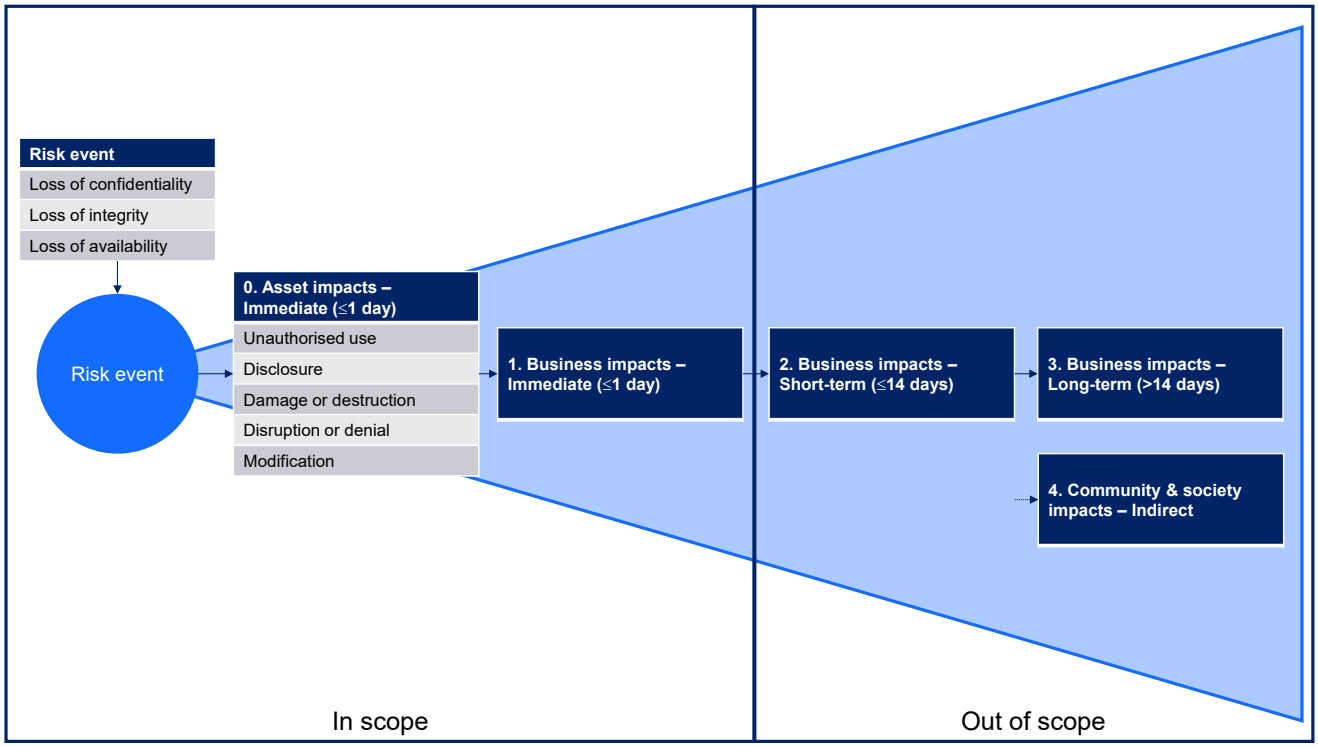


Figure 3 – Relationship and development of asset and business impacts over time

- The timeframe for a business impact to be considered direct and immediate shall be within one calendar day.
- The business impact scenarios shall be developed and expressed using all applicable risk management frameworks and criteria.

Note: The expression of business impacts against multiple frameworks and criteria allows for the articulation of Transport cluster and operating agency or entity viewpoints of the asset's criticality.

- The risk criteria shall include the following:
  - Transport risk criteria defined in either TS 04982 or CPSt20000
  - operating agency or entity risk criteria

Note: CPSt20000 applies to stated agencies within Transport. TS 04982 applies to all TAOs or organisations providing engineering services for TfNSW. TS 04982 aligns with the TfNSW enterprise risk management framework set out in CPSt20000.

- The business impact scenarios shall include causal impacts on dependant systems.
- For the purpose of this procedure, the business impact scenarios are not required to include direct impacts beyond the operational window of one calendar day or indirect impacts as shown in Figure 3.

  Note: Business impact assessments consider the direct short-term impacts within a window of 14 days as part of business continuity planning.

6.2.3 Data outputs

Data outputs from this task include the following:

- descriptive business impact scenarios for system and main parts of the system.

6.3 Task 1.3: Assess business impact scenarios

The purpose of this task is to assess the consequence rating of business impact scenarios.

6.3.1 Data inputs

Data inputs to this task include the following:

- descriptive business impact scenarios for system and main parts of the system.

6.3.2 Task procedure

The steps for this task shall be performed as follows:

1. Rate the credible worst-case consequence of each identified business impact scenario using the applicable risk criteria:
    a. The consequence of a risk event shall be assessed against all applicable risk categories.
    b. The credible worst-case consequence shall include the direct and immediate impacts of the risk event only.

    Figure 4 and Figure 5 show simplified example scenarios of a smart ticketing system data breach and an altered intelligent transportation systems configuration. These figures have been included to provides examples of the direct and immediate impacts which are in scope; and short and long-term impacts and indirect impacts which are out of scope.

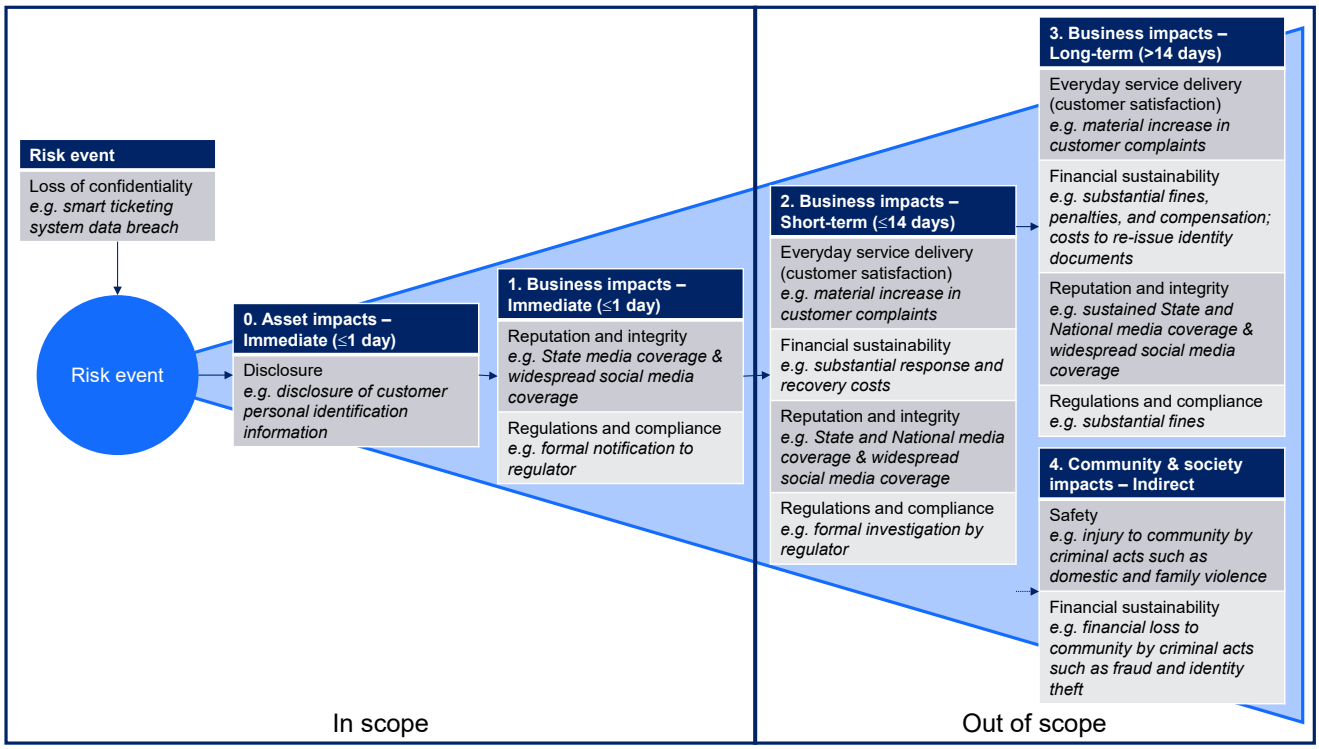


Figure 4 – Example scenario: Smart ticketing system data breach

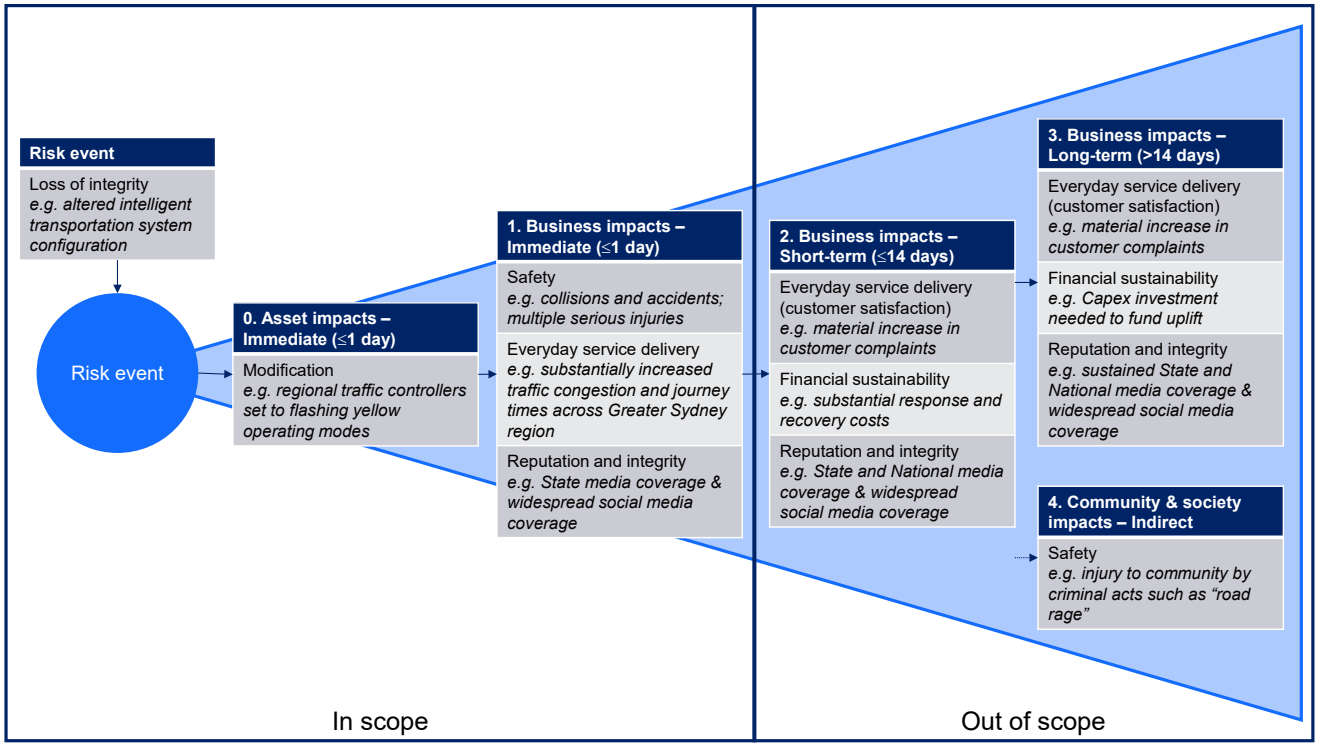


Figure 5 – Example scenario: Altered intelligent transportation systems configuration

c. The worst-case consequence shall include mitigations associated with the reasonable application of incident response and disaster recovery plans.

d. To include mitigations associated with the reasonable application incident response and disaster recovery plans they shall satisfy the following criteria:

- plans are adopted, maintained, regularly reviewed, and updated
- plans are regularly tested by cyber security exercises.

6.3.3 Data outputs

Data outputs from this task include the following:

- assessed business impact scenarios for system and main parts of the system.

6.4 Task 1.4: Determine preliminary criticality

The purpose of this task is to determine the preliminary criticality of the system and parts of the system.

6.4.1 Data inputs

Data inputs to this task include the following:

- assessed business impact scenarios for system and main parts of the system.

6.4.2 Task procedure

The steps for this task shall be performed as follows:

1. Determine the Transport or asset custodian criticality level from Table 3 using the highest consequence rating of all business impact scenarios using the Transport risk criteria.

   Note: This provides a consistent Transport-wide view of asset criticality which supports asset custodians in making informed investment decisions.

Table 3 – Criticality levels

Consequence rating	Risk categories	Criticality level
C1 Catastrophic	Safety, Environment, Everyday Service Delivery, Regulation and Compliance	CL1 Mission-critical
C1 Catastrophic	Any other categories	CL2 Critical
C2 Severe	Any categories	CL3 High
C3 Major	Any categories	CL4 Medium
C4 Moderate	Any categories	CL5 Low
C5 Minor	Any categories	CL5 Low
C6 Insignificant	Any categories	CL5 Low

2. Determine the asset steward criticality level using the highest consequence rating of all business impact scenarios using the operating agency or entity risk criteria.

Note: This provides an operating agency or entity view of asset criticality which supports operational decision-making.

- The asset steward shall produce a mapping between the operating agency or entity risk criteria and the five criticality levels CL1 to CL5.

3. Determine whether information and cyber security compliance obligations apply to the system using Appendix A.

   Note: In addition to information and cyber security compliance obligations, standards may set requirements for technology systems based on the assessed criticality level.

4. Record the criticality levels using the TS 00087.2 form.

6.4.3 Data outputs

Data outputs from this task include the following:

- preliminary criticality assessment.

7 Task 2: Finalise assessment

An overview of the task is shown in Figure 6.

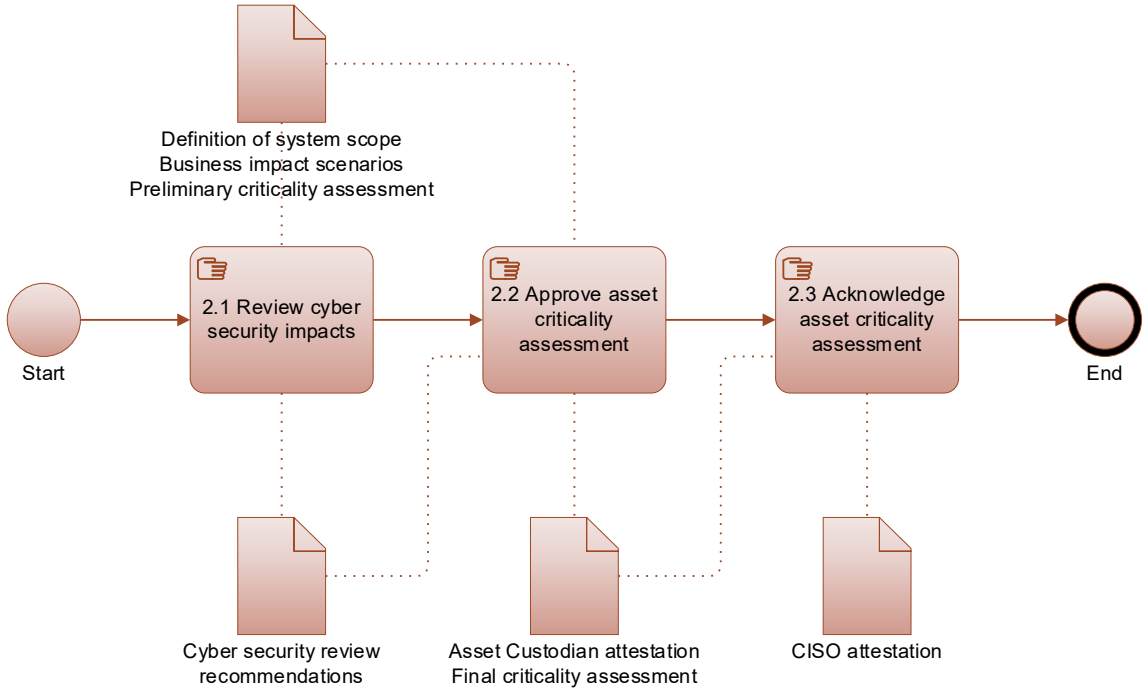


Figure 6 – Task 2: Finalise assessment procedure

The governance steps to finalise the assessment are summarised in Table 4.

Table 4 – Summary of governance steps

Role	Action	Attestation
TCD Advisory	Review	Nil – recommendations only.
Asset Custodian	Approve	• the procedure set out in this document has been followed • all relevant stakeholders have been identified and consulted • the scope of the system has been accurately defined • the business impacts of the loss of confidentiality, integrity, and availability for the system and main parts of the system have been identified and assessed • the asset criticality level accurately reflects the importance of the system to TfNSW in the achievement of agreed customer and community outcomes.

Role	Action	Attestation
CISO	Acknowledge	• any changes to the applicability of TfNSW information and cyber security compliance obligations are accepted on behalf of TfNSW • the system will be onboarded to or offboarded from TfNSW information and cyber security management system as applicable.

7.1 Task 2.1: Review cyber security impacts

The purpose of this task is for TCD Advisory to review the criticality assessment to ensure that the business impact assessment for the system is credible from a cyber security perspective.

7.1.1 Data inputs

Data inputs to this task include the following:

- definition of system scope
- business impact assessment for system and main parts of the system
- preliminary criticality assessment.

7.1.2 Task procedure

The steps for this task shall be performed as follows:

1. The asset custodian shall engage TCD Advisory to review the preliminary criticality assessment.

   Note: TCD Advisory can be engaged using the Critical Asset Identification Service on MyTransport.

2. TCD Advisory shall independently review and make recommendations to the asset custodian whether to approve, approve with changes or conditions, or reject the preliminary criticality assessment developed by the asset steward.

   Note: Where TCD Advisory has been previously engaged to support the development of the preliminary criticality assessment appropriate measures will be taken to manage conflicts of interest.

7.1.3 Data outputs

Data outputs from this task include the following:

- recommendations from TCD Advisory.

7.2 Task 2.2: Approve asset criticality assessment

The purpose of this task is for the asset custodian to review and approve the criticality assessment on behalf of the asset owner to ensure the achievement of agreed customer and community outcomes.

7.2.1 Data inputs

Data inputs to this task include the following:

- preliminary criticality assessment
- recommendations from TCD Advisory.

7.2.2 Task procedure

The steps for this task shall be performed as follows:

1. The asset custodian shall review and determine whether to approve, approve with changes or conditions, or reject the preliminary criticality assessment developed by the asset steward.
    a. In approving the assessment, the asset custodian is attesting to all the following:
        - the procedure set out in this document has been followed
        - all relevant stakeholders have been identified and consulted
        - the scope of the system has been accurately defined
        - the business impacts of the loss of confidentiality, integrity, and availability for the system and main parts of the system have been identified and assessed
        - the asset criticality level accurately reflects the importance of the system to TfNSW in the achievement of agreed customer and community outcomes.

7.2.3 Data outputs

Data outputs from this task include the following:

- final criticality assessment
- asset custodian attestation.

7.3 Task 2.3: Acknowledge asset criticality assessment

The purpose of this task is to ensure that where the final criticality assessment results in changes to the applicability of TfNSW information and cyber security compliance obligations, the CISO acknowledges and accepts these obligations on behalf of TfNSW.

7.3.1 Data inputs

Data inputs to this task include the following:

- final criticality assessment.

7.3.2 Task procedure

The steps for this task shall be performed as follows:

1. The asset custodian shall notify TCD Compliance of the final criticality assessment.
2. TCD Compliance shall facilitate the formal acknowledgement of the final criticality assessment and acceptance of changes to the applicability of TfNSW information and cyber security compliance obligations.
    a. In acknowledging the assessment, the CISO supported by CDPB is attesting to all the following:
        - any changes to the applicability of TfNSW information and cyber security compliance obligations are accepted on behalf of TfNSW
        - the system will be onboarded to or offboarded from TfNSW information and cyber security management system as applicable.

7.3.3 Data outputs

Data outputs from this task include the following:

- CISO attestation.

8 Task 3: Onboard system

The purpose of this task is to onboard the system to the TfNSW information and cyber security management system.

8.1.1 Data inputs

Data inputs to this task include the following:

- definition of system scope
- final criticality assessment.

8.1.2 Task procedure

The steps for this task shall be performed as follows:

1. Onboard the system to the TfNSW information and cyber security management system.

8.1.3 Data outputs

Data outputs from this task include the following:

- record in TfNSW information and cyber security management system.

9 Task 4: Offboard system

The purpose of this task is to offboard the system from the TfNSW information and cyber security management system.

9.1.1 Data inputs

Data inputs to this task include the following:

- definition of system scope
- final criticality assessment.

9.1.2 Task procedure

The steps for this task shall be performed as follows:

1. Offboard the system from the TfNSW information and cyber security management system.

9.1.3 Data outputs

Data outputs from this task include the following:

- nil.

Appendix A Mappings to other criticality frameworks (normative)

This appendix sets out mappings between the criticality levels and other criticality frameworks.

A.1 Mapping to NSW CSP

Systems assessed with a criticality level of ‘CL1 mission-critical’ shall be deemed a crown jewel for the purpose of the NSW CSP.

Appendix B Example preliminary criticality assessment

B.1 Example operational radio system

A digital train radio system (DTRS) is an operational radio system that facilitates voice and data communications throughout the metropolitan railway networks (inclusive of yards and sidings), train control and signalling facilities as well as rolling stock.

DTRS is chosen as the system under consideration for this example.

> Note: This content in this example is fictitious. No identification with actual systems is intended or should be inferred.

B.1.1 Task 1.1: Determine system scope

Figure 7 shows the high-level scope of the system which including include all computers, computer systems, and computer networks within the system under consideration for this assessment.

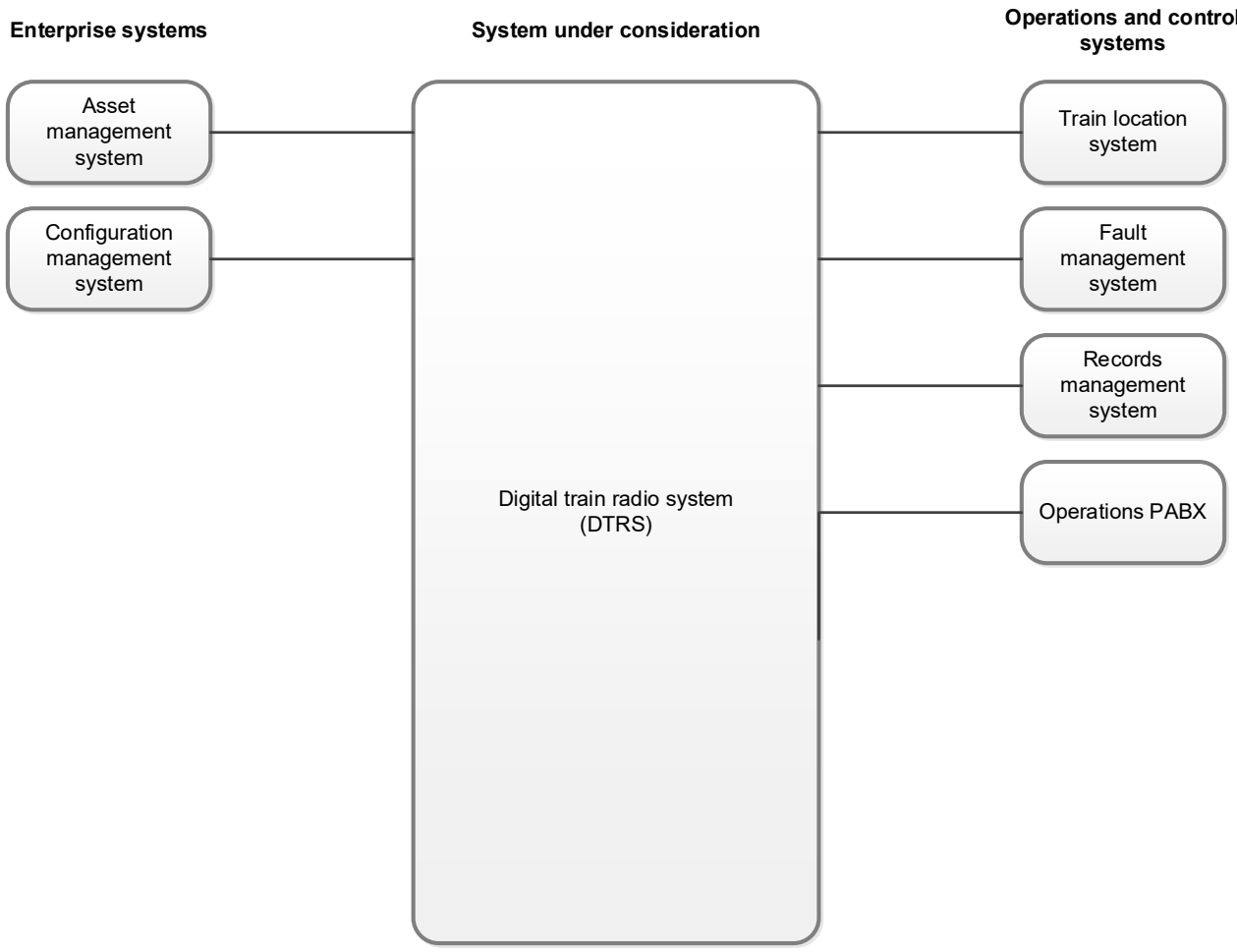


Figure 7 – High-level scope of the system

Figure 8 shows the main parts of the system and their physical and logical security perimeters and access points:

- The physical security perimeter is represented as ‘sites’ and depicted using round-edged rectangles with solid lines.
- The logical security perimeter is represented as wide area networks (WAN) and local area networks (LAN).
- In this example, LANs are trusted and are depicted as white conduits, while WANs are untrusted and are depicted as dark grey conduits.

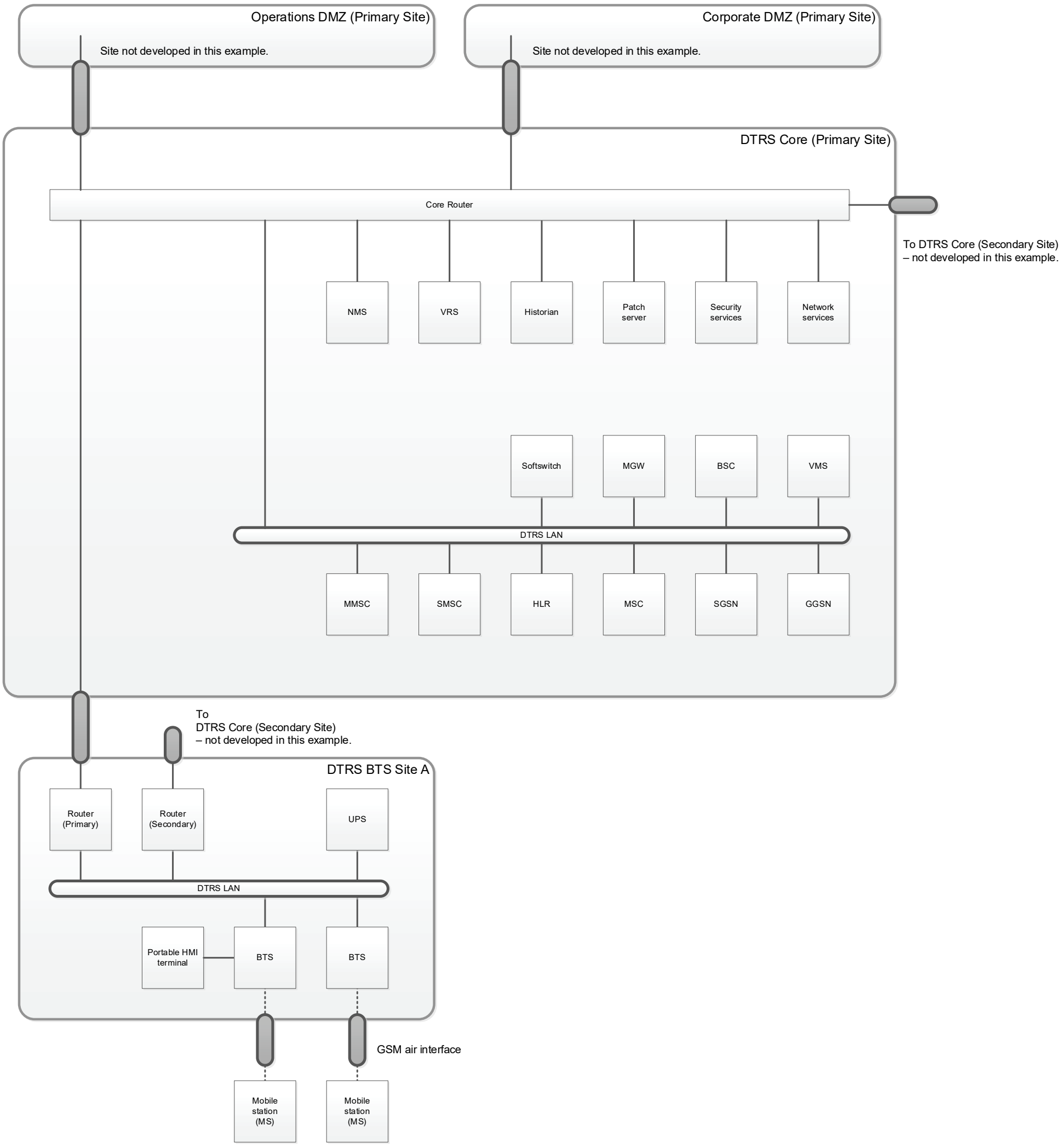


Figure 8 – Security perimeter and access points

B.1.2 Task 1.2: Identify business impact scenarios

This example uses a textual format to describe business impact scenarios as follows:

Scenario # *scenario description*

In the (*system or part of system*) the (*risk event*) may have the following asset impacts: (*asset impacts*). This may result in the following direct and immediate business impacts: (*consequence category*) – (*consequence description*).

A completed example of a business impact scenario using the Transport risk criteria is as follows:

Scenario #1 Complete operational radio system failure

In the DTRS the complete operational radio system failure (loss of availability) may have the following asset impacts:

- disruption or denial – loss of operational communications and loss of railway emergency calls

This may result in the following direct and immediate business impacts:

- safety – delays in provision of medical treatment
- everyday service delivery – shutdown of a mode of transport; degraded mode of operations
- reputation and integrity – State media coverage and widespread social media coverage
- regulations and compliance – formal notification to regulators

This example can also be presented visually as shown in Figure 9.

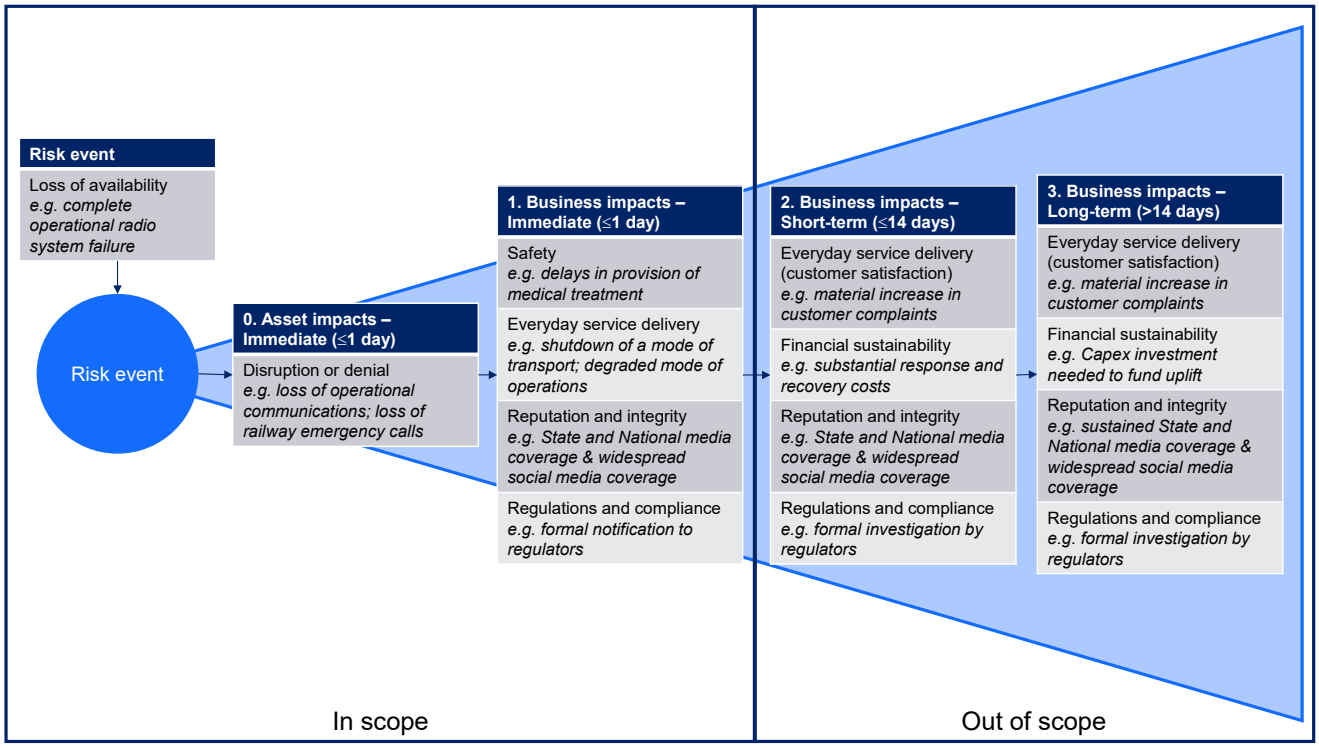
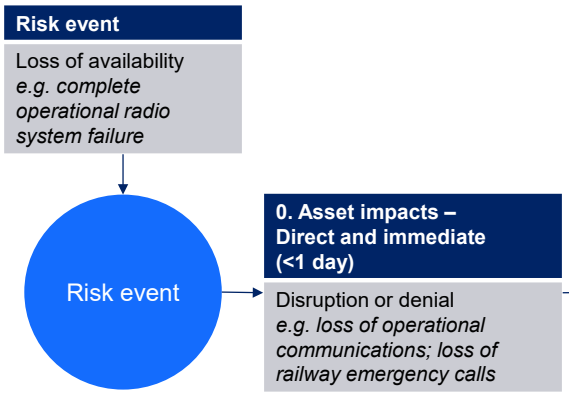


Figure 9 – Task 1.2: Scenario #1 Complete operational radio system failure

B.1.3 Task 1.3: Assess business impact scenarios

A completed example of a business impact scenario assessed using both the Transport and operating agency or entity risk criteria is shown in Figure 10.



1. Business impacts – Immediate (≤1 day) (Transport)	1. Business impacts – Immediate (≤1 day) (Asset Steward)
Safety *e.g. delays in provision of medical treatment –* **C4 Moderate**	Safety / Health *e.g. delays in provision of medical treatment –* **C3 Moderate**
Everyday service delivery *e.g. shutdown of a mode of transport; degraded mode of operations –* **C3 Major**	Customer Experience and Operational Performance *e.g. shutdown of a mode of transport for a multiple peak periods; degraded mode of operations –* **C6 Catastrophic**
Reputation and integrity *e.g. State and National media coverage & widespread social media coverage –* **C2 Severe**	Reputation *e.g. Sustained national media coverage & extensive stakeholder concern –* **C5 Severe**
Regulations and compliance *e.g. formal notification to regulators –* **C4 Moderate**	Regulations and compliance *e.g. formal notification to regulators –* Refer to 'Reputation'

Figure 10 – Task 1.3: Scenario #1 Complete operational radio system failure

B.1.4 Task 1.4: Determine preliminary criticality

The Transport or asset custodian criticality level is ‘CL3 High’.

The asset steward criticality level is ‘CL1 Mission-critical’.

In this example, DTRS would be deemed a crown jewel from the viewpoint of the operating agency or entity for the purpose of the NSW CSP.